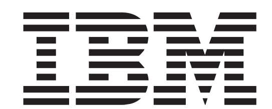
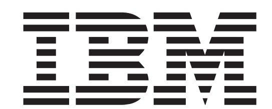
IBM Client Security Solutions



Client Security Version 5.1 Administratorhandbuch

IBM Client Security Solutions



Client Security Version 5.1 Administratorhandbuch

Hinweis:

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang C, „Bemerkungen und Marken", auf Seite 79, lesen.

Erste Ausgabe (April 2003)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions, Client Security Version 5.1 Administrator's Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
April 2003

Inhaltsverzeichnis

Vorwort

Dieses Handbuch enthält Informationen zur Konfiguration und zur Verwendung der Sicherheitsfunktionen von Client Security.

Das Handbuch ist wie folgt aufgebaut:

Kapitel 1, „**Einführung in IBM Client Security**”, enthält eine Übersicht über die Anwendungen und Komponenten der Software sowie eine Beschreibung der PKI-Funktionen.

Kapitel 2, „Verschlüsselung von Dateien und Ordnern”, enthält Informationen zur Verwendung von Client Security für den Schutz sensibler Dateien und Ordner.

Kapitel 3, „Client Security verwenden”, enthält Beispiele für die Verwendung von Client Security-Komponenten für die Konfiguration der von Clientbenutzern benötigten Sicherheitseinrichtungen.

Kapitel 4, „Benutzer autorisieren”, enthält Informationen zur Authentifizierung von Clientbenutzern und erläutert das Autorisieren und Entfernen von Benutzern im User Verification Manager (UVM).

Kapitel 5, „Nach dem Hinzufügen von Benutzern in UVM”, enthält Anweisungen zum Einrichten des UVM-Schutzes für die Betriebssystemanmeldung, zur Verwendung des UVM-Schutzes für Lotus Notes und zur Verwendung von Client Security mit Netscape-Anwendungen.

Kapitel 6, „Mit der UVM-Policy arbeiten”, enthält Anweisungen zum Bearbeiten einer lokalen UVM-Policy, zur Verwendung einer UVM-Policy für einen fernen Client und zum Ändern des Kennworts für eine UVM-Policy-Datei.

Kapitel 7, „Weitere Funktionen des Sicherheitsadministrators”, enthält Anweisungen zum Ändern der Speicherposition des Schlüsselarchivs, zum Wiederherstellen eines UVM-Verschlüsselungstextes und zum Aktivieren oder Inaktivieren des integrierten IBM Security Chips mit Hilfe des Administratordienstprogramms.

Kapitel 8, „Anweisungen für den Clientbenutzer”, enthält Anweisungen zu unterschiedlichen Tasks, die der Clientbenutzer mit Client Security ausführen kann. Dazu gehören Anweisungen zur Verwendung der gesicherten UVM-Anmeldung, des Client Security-Bildschirmschoners, der sicheren E-Mail-Übertragung und des Benutzerkonfigurationsprogramms.

Kapitel 9, „Fehlerbehebung”, enthält nützliche Informationen zum Umgehen bekannter Einschränkungen und Fehler, die möglicherweise beim Befolgen der Anweisungen in diesem Handbuch auftreten.

Anhang A, „Regeln für Kennwörter und Verschlüsselungstexte”, enthält Kriterien für Kennwörter, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Kennwörter für den IBM Security Chip.

Anhang B, „Regeln für den UVM-Schutz für die Anmeldung am System”, enthält Informationen zur Verwendung des UVM-Schutzes für die Anmeldung am Betriebssystem.

Anhang C, „Bemerkungen und Marken”, enthält rechtliche Hinweise und Informationen zu Marken.

Zielgruppe

Dieses Handbuch ist für Sicherheitsadministratoren bestimmt, die folgende Vorgänge durchführen:

- Benutzerauthentifizierung für den IBM Client konfigurieren
- UVM-Sicherheits-Policy für IBM Clients konfigurieren und bearbeiten
- Mit dem Administratordienstprogramm das Sicherheitssubsystem (den integrierten IBM Security Chip) und den einzelnen IBM Clients zugeordnete Einstellungen verwalten.

Dieses Handbuch ist außerdem für Tivoli Access Manager-Administratoren konzipiert, die mit IBM Tivoli Access Manager-Authentifizierungsobjekte verwalten, die sich in der UVM-Policy befinden. Tivoli Access Manager-Administratoren müssen Folgendes verwalten können:

- Objektbereich von Tivoli Access Manager
- Prozesse für die Authentifizierung, die Autorisierung und die Anforderung des Berechtigungsnachweises
- IBM Umgebung mit verteilter Datenverarbeitung (IBM Distributed Computing Environment - DCE)
- Protokoll ″LDAP″ (Lightweight Directory Access Protocol) von IBM SecureWay Directory

Benutzung des Handbuchs

Mit diesem Handbuch können Sie die Benutzerauthentifizierung und die UVM-Sicherheits-Policy für IBM Clients konfigurieren. Es wird ergänzt durch das *Client Security Installationshandbuch*, das Handbuch *Client Security mit Tivoli Access Manager verwenden* und das *Client Security Benutzerhandbuch*. Das vorliegende Handbuch und die gesamte Dokumentation zu Client Security kann von der IBM Website unter http://www.pc.ibm.com/ww/security/secdownload.html heruntergeladen werden.

Verweise auf das *Client Security Installationshandbuch*

In diesem Dokument finden Sie Verweise auf das *Client Security Installationshandbuch*. Sie müssen Client Security auf einem IBM Client installieren, bevor Sie das vorliegende Handbuch verwenden können. Anweisungen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.

Verweise auf das Handbuch *Client Security mit Tivoli Access Manager verwenden*

In diesem Dokument finden Sie Verweise auf das Handbuch *Client Security mit Tivoli Access Manager verwenden*. Sicherheitsadministratoren, die mit Tivoli Access Manager Authentifizierungsobjekte für die UVM-Policy verwalten, sollten das Handbuch *Client Security mit Tivoli Access Manager verwenden* lesen.

Verweise auf das *Client Security Benutzerhandbuch*

In diesem Dokument finden Sie Verweise auf das *Client Security Benutzerhandbuch*. Administratoren können mit diesem Handbuch UVM-Policies auf IBM Clients, auf denen Client Security eingesetzt wird, verwalten und warten. Nachdem ein Administrator die Benutzerauthentifizierung und die UVM-Sicherheits-Policy konfiguriert hat, kann ein Clientbenutzer im *Client Security Benutzerhandbuch* Informationen zu Client Security lesen.

Das Benutzerhandbuch enthält Informationen zur Ausführung von Arbeiten mit Client Security, wie z. B. zur gesicherten UVM-Anmeldung, zur Konfiguration des Client Security-Bildschirmschoners, zur Erstellung eines digitalen Zertifikats und zur Verwendung des Benutzerkonfigurationsprogramms.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können Sie, sobald sie verfügbar sind, von der IBM Website unter

http://www.pc.ibm.com/ww/security/index.html

herunterladen.

Kapitel 1. Einführung in IBM Client Security

Die Software ″IBM Client Security″ ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und Speichern von Chiffrierschlüsseln verwenden. Client Security besteht aus Anwendungen und Komponenten, mit denen IBM Kunden die Sicherheit von Clients im lokalen Netzwerk, im Unternehmen oder im Internet gewährleisten können.

Anwendungen und Komponenten von Client Security

Wenn Sie Client Security installieren, werden die folgenden Softwareanwendungen und -komponenten installiert:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, über die ein Administrator den integrierten IBM Security Chip aktiviert oder inaktiviert sowie Chiffrierschlüssel und Verschlüsselungstexte erstellt, archiviert und erneut generiert. Darüber hinaus kann ein Administrator mit diesem Dienstprogramm der Sicherheits-Policy, die von Client Security bereitgestellt wird, Benutzer hinzufügen.
- **User Verification Manager (UVM):** In Client Security werden mit UVM Verschlüsselungstexte und andere Elemente verwaltet, mit denen Systembenutzer authentifiziert werden. Mit einem Lesegerät für Fingerabdrücke kann UVM z. B. bei der Anmeldung Benutzer authentifizieren. UVM bietet folgende Möglichkeiten:
  - **Schutz durch UVM-Client-Policy:** Mit UVM kann ein Administrator die Sicherheits-Policy für Clients festlegen, die bestimmt, wie auf dem System die Authentifizierung eines Clientbenutzers erfolgt.

    Wenn die Policy festlegt, dass Fingerabdrücke für die Anmeldung erforderlich sind, und der Benutzer keine Fingerabdrücke registriert hat, hat er die Möglichkeit, Fingerabdrücke bei der Anmeldung zu registrieren. Wenn die Überprüfung von Fingerabdrücken erforderlich ist und kein Scanner angeschlossen ist, meldet UVM einen Fehler. Wenn das Windows-Kennwort nicht oder nicht richtig in UVM registriert ist, hat der Benutzer die Möglichkeit, das richtige Windows-Kennwort als Teil der Anmeldung anzugeben.
  - **UVM-Systemanmeldeschutz:** UVM ermöglicht es Administratoren, den Zugriff auf die Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheits-Policy erkannt werden, auf das Betriebssystem zugreifen können.
  - **UVM Client Security-Bildschirmschonerschutz:** Bei Einsatz von UVM können Benutzer den Zugriff auf den Computer über eine Schnittstelle für den Client Security-Bildschirmschoner steuern.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht es einem Sicherheitsadministrator, administratorspezifische Tasks über Fernzugriff auszuführen.
- **Benutzerkonfigurationsprogramm:** Mit dem Benutzerkonfigurationsprogramm können Clientbenutzer den UVM-Verschlüsselungstext ändern. Unter Windows 2000 und Windows XP können Benutzer mit dem Clientdienstprogramm Schlüsselarchive aktualisieren und Windows-Anmeldekennwörter ändern, so dass diese von UVM erkannt werden. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Security Chip erzeugt wurden.

PKI-Funktionen

Client Security bietet alle erforderlichen Komponenten, um in Ihrem Unternehmen eine PKI (Public Key Infrastructure) aufzubauen, z. B.:

- **Steuerung der Client-Sicherheits-Policy durch Administratoren:** Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt für Sicherheits-Policies. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheits-Policy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für öffentliche Schlüssel:** Administratoren können mit Client Security Chiffrierschlüssel für die Computerhardware und für die Clientbenutzer erstellen. Bei der Erstellung von Chiffrierschlüsseln sind diese über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. In der Hierarchie wird ein Hardwareschlüssel der Basisebene verwendet, um die übergeordneten Schlüssel sowie die den einzelnen Clientbenutzern zugeordneten Benutzerschlüssel zu verschlüsseln. Die Verschlüsselung und Speicherung von Schlüsseln auf dem integrierten IBM Security Chip erweitert die Clientsicherheit um eine wesentliche zusätzliche Ebene, da die Schlüssel sicher an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Signaturen, die durch den integrierten IBM Security Chip geschützt sind:** Wenn Sie ein digitales Zertifikat anfordern, das für die digitale Signatur und für die Verschlüsselung einer E-Mail verwendbar ist, können Sie mit Client Security den integrierten IBM Security Chip zur Bereitstellung der Verschlüsselung für Anwendungen einsetzen, die mit der Microsoft CryptoAPI funktionieren. Zu diesen Anwendungen gehören Internet Explorer und Microsoft Outlook Express. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem integrierten IBM Security Chip gespeichert wird. Darüber hinaus können Netscape-Benutzer integrierte IBM Security Chips zum Generieren von privaten Schlüsseln für die zum Erhöhen der Systemsicherheit verwendeten digitalen Zertifikate auswählen. Anwendungen nach dem Standard PKCS #11 (Public-Key Cryptography Standard Nr. 11), wie z. B. Netscape Messenger, können sich über den integrierten IBM Security Chip schützen.
- **Digitale Zertifikate auf den integrierten IBM Security Chip übertragen:** Mit dem Tool zur Übertragung von Zertifikaten von Client Security können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen. Dadurch wird der notwendige Schutz für private Schlüssel, die zu Zertifikaten gehören, beträchtlich erhöht, da die Schlüssel nun statt in gefährdeter Software im integrierten IBM Security Chip sicher gespeichert sind.
- **Funktion zur Schlüsselarchivierung und -wiederherstellung:** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, aus dem Schlüssel bei Verlust oder Beschädigung der Originalschlüssel wiederhergestellt werden können. Client Security bietet eine Schnittstelle, mit der Sie mit dem integrierten IBM Security Chip erstellte Archive für Schlüssel und digitale Zertifikate erstellen und diese Schlüssel und Zertifikate bei Bedarf wiederherstellen können.
- **Verschlüsselung von Dateien und Ordnern:** Die Verschlüsselung von Dateien und Ordnern ermöglicht dem Benutzer das schnelle und einfache Ver- und Entschlüsseln von Dateien und Ordnern. So wird eine höhere Stufe von Datensicherheit als erste der Sicherheitsmaßnahmen des CSS-Systems gewährleistet.

- **Authentifizierung über Fingerabdrücke:** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Die Client Security-Software muss installiert sein, bevor die Einheitentreiber für das Targus-Lesegerät für Fingerabdrücke installiert werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist.
- **Smartcard-Authentifizierung:** IBM Client Security unterstützt jetzt auch Smartcards als Authentifizierungseinheiten. Client Security ermöglicht die Verwendung von Smartcards zur Authentifizierung als Token, d. h., es kann sich jeweils nur ein Benutzer authentifizieren. Jede Smartcard ist systemgebunden, wenn nicht der standortunabhängige Zugriff (Roaming) mit Berechtigungsnachweis verwendet wird. Wenn eine Smartcard erforderlich ist, sollte die Systemsicherheit erhöht werden, da diese Karte mit einem Kennwort geliefert werden muss, das möglicherweise ausspioniert werden kann.
- **Standortunabhängiger Zugriff mit Berechtigungsnachweis:** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem von UVM autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei CSS registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem System, in das sie importiert wurden, automatisch aktualisiert und gewartet. Aktualisierungen der persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen am Verschlüsselungstext, sind sofort auf allen Systemen verfügbar.
- **FIPS 140-1-Zertifizierung:** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken. FIPS-zertifizierte RSA-BSAFE-Bibliotheken werden auf TCPA-Systemen verwendet.
- **Ablauf des Verschlüsselungstexts:** Client Security legt jeweils beim Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.
- **Automatischer Schutz für ausgewählte Ordner:** Die Funktion zum automatischen Schützen von Ordnern ermöglicht es einem Client-Security-Administrator, festzulegen, dass alle Ordner mit der Bezeichnung "Eigene Dateien" der von UVM autorisierten Benutzer automatisch geschützt werden, ohne dass seitens der Benutzer eine Aktivität ausgeführt werden muss.

Kapitel 2. Verschlüsselung von Dateien und Ordnern

Das Dienstprogramm zur Verschlüsselung von Dateien und Ordnern, das von der Website für IBM Client Security heruntergeladen werden kann, ermöglicht es Benutzern, sensible Dateien und Ordner durch Klicken mit der rechten Maustaste zu verschlüsseln. Art und Umfang des durch die Verschlüsselung erzielten Schutzes richten sich nach der beim Verschlüsseln der Datei bzw. des Ordners angewandten Vorgehensweise. Anhand der folgenden Informationen können Sie bestimmen, welche Verschlüsselungstechnik Sie zum Schutz Ihrer Daten anwenden sollten. IBM Client Security muss *vor* der Installation des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern installiert werden.

Das Dienstprogramm zur Plattenüberprüfung wird möglicherweise bei einem Neustart nach dem Schützen oder dem Aufheben des Schutzes von Ordnern ausgeführt. Warten Sie, bis das System geprüft ist, bevor Sie den Computer verwenden.

Dateischutz durch Klicken mit der rechten Maustaste

Sie können Dateien im Kontextmenü mit der rechten Maustaste manuell ver- und entschlüsseln. Wenn Sie Dateien auf diese Weise verschlüsseln, wird an den Dateinamen die Erweiterung .enc angehängt. Diese verschlüsselten Dateien können Sie anschließend auf fernen Servern sicher speichern. Sie bleiben so lange verschlüsselt und für Anwendungen nicht verfügbar, bis Sie sie mit der rechten Maustaste wieder entschlüsseln.

Ordnerschutz durch Klicken mit der rechten Maustaste

Ein in UVM registrierter Benutzer kann einen Ordner auswählen, um den Ordner mit der rechten Maustaste zu schützen oder den Schutz aufzuheben. Dadurch kann er alle Dateien innerhalb des Ordners oder alle untergeordneten Teilordner verschlüsseln. Wenn Sie Dateien auf diese Weise schützen, wird an deren Namen keine Erweiterung angehängt. Wenn Sie mit einer Anwendung auf eine Datei im verschlüsselten Ordner zugreifen, wird diese entschlüsselt, in den Speicher geladen und erneut verschlüsselt, bevor Sie sie auf der Festplatte speichern.

Alle Windows-Operationen, die auf eine Datei in einem geschützten Ordner zuzugreifen versuchen, erhalten Zugriff auf die Daten in entschlüsselter Form. Diese Funktion steigert die Benutzerfreundlichkeit, so dass Sie eine Datei vor ihrer Verwendung nicht entschlüsseln und nach der Verarbeitung durch ein Programm nicht erneut verschlüsseln müssen.

Status der Ordnerverschlüsselung

Mit Client Security können Benutzer mit der rechten Maustaste sensible Dateien und Ordner schützen. Die Art des Datei- oder Ordnerschutzes hängt von der ursprünglichen Verschlüsselung der Datei bzw. des Ordners ab.

Ein Ordner kann sich in einem der folgenden Status befinden, wobei jeder Status unterschiedlich behandelt wird, wenn Sie die rechte Maustaste für Ordner verwenden:

- **Ungeschützter Ordner**

  Weder dieser Ordner noch seine Teilordner noch einer seiner übergeordneten Ordner wurde geschützt. Der Benutzer erhält die Option, diesen Ordner zu schützen.
- **Geschützter Ordner**

  Ein geschützter Ordner kann sich in einem der folgenden drei Status befinden:
  - **Vom aktuellen Benutzer geschützt**

    Der aktuelle Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern. Der Benutzer erhält die Option, den Schutz dieses Ordners aufzuheben.
  - **Vom aktuellen Benutzer geschützter Teilordner eines Ordners**

    Der aktuelle Benutzer schützt einen der übergeordneten Ordner dieses Ordners. Alle Dateien werden verschlüsselt. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.
  - **Von einem anderen Benutzer geschützt**

    Ein anderer Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern, und sie sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.
- **Übergeordneter Ordner eines geschützten Ordners**

  Ein übergeordneter Ordner eines geschützten Ordners kann sich in einem der folgenden drei Status befinden:
  - **Enthält mindestens einen Teilordner, der vom aktuellen Benutzer geschützt wurde**

    Der aktuelle Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt. Der Benutzer erhält die Option, den übergeordneten Ordner zu schützen.
  - **Enthält mindestens einen Teilordner, der von mindestens einem anderen Benutzer geschützt wurde**

    Mindestens ein anderer Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt und sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.
  - **Enthält Teilordner, die vom aktuellen Benutzer und von mindestens einem anderen Benutzer geschützt wurden**

    Sowohl der aktuelle Benutzer als auch mindestens ein anderer Benutzer schützen Teilordner. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.
- **Kritischer Ordner**

  Ein kritischer Ordner ist ein Ordner in einem kritischen Pfad und kann daher nicht geschützt werden. Es gibt die beiden folgenden kritischen Pfade: den Pfad von Windows und den Pfad von Client Security.

Jeder Status wird von der Option zum Schützen eines Ordners durch Klicken mit der rechten Maustaste unterschiedlich gehandhabt.

Hinweise zur Verwendung des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern (Dienstprogramm ″FFE″, File and Folder Encryption)

Die folgenden Informationen sind möglicherweise nützlich, wenn Sie bestimmte Funktionen zur Verschlüsselung von Dateien und Ordnern durchführen.

Laufwerkbuchstabenschutz

Das IBM Dienstprogramm ″FFE″ kann ausschließlich zum Verschlüsseln von Dateien und Ordnern auf Laufwerk C verwendet werden. Dieses Dienstprogramm unterstützt keine Verschlüsselung auf anderen Festplattenpartitionen oder anderen physischen Laufwerken.

Geschützte Dateien und Ordner löschen

Damit sich keine sensiblen Dateien und Ordner ungeschützt im Papierkorb befinden, cmüssen Sie die Tastenkombination Umschalttaste+Entf verwenden, um geschützte Ordner und Dateien zu löschen. Durch diese Tastenkombination wird eine nicht an Bedingungen gebundene Löschoperation durchgeführt, und die gelöschten Dateien werden nicht im Papierkorb abgelegt.

Vor dem Upgrade von einer älteren Version des Dienstprogramms ″IBM FFE″

Wenn Sie von einer älteren Version des Dienstprogramms ″IBM FFE″ (Version 1.04 oder älter) aufrüsten möchten und sich die geschützten Ordner auf anderen Laufwerken als Laufwerk C befinden, heben Sie den Schutz für diese Ordner auf, bevor Sie Version 1.05 des Dienstprogramms ″IBM FFE″ installieren. Wenn Sie nach dem Installieren von Version 1.05 diese Ordner erneut schützen müssen, verschieben Sie sie auf Laufwerk C, und schützen Sie sie.

Vor dem Deinstallieren des Dienstprogramms ″IBM FFE″

Heben Sie vor dem Deinstallieren des Dienstprogramms ″IBM FFE″ mit Hilfe dieses Dienstprogramms den Schutz für alle zuvor geschützten Dateien und Ordner auf.

Einschränkungen beim Dienstprogramm zur Verschlüsselung von Dateien und Ordnern (Dienstprogramm ″FFE″)

Das Dienstprogramm ″IBM FFE″ weist folgende Einschränkungen auf:

Einschränkungen beim Verschieben von geschützten Dateien und Ordnern

Das Dienstprogramm ″IBM FFE″ unterstützt folgende Aktionen nicht:

- Dateien und Ordner innerhalb geschützter Ordner verschieben
- Dateien oder Ordner zwischen geschützten und ungeschützten Ordnern verschieben

Wenn Sie versuchen, eine dieser nicht unterstützten Verschiebeoperationen durchzuführen, wird vom Betriebssystem eine Nachricht angezeigt, die besagt, dass der Zugriff verweigert wurde. Dies ist ein normaler Vorgang. Die Nachricht besagt lediglich, dass diese Verschiebeoperation nicht unterstützt wird. Alternativ zur Verschiebeoperation können Sie folgende Operation ausführen:

1. Kopieren Sie die geschützten Dateien oder Ordner an die neue Position.
2. Löschen Sie die ursprünglichen Dateien oder Ordner mit Hilfe der Tastenkombination Umschalttaste+Entf.

Einschränkungen beim Ausführen von Anwendungen

Das Dienstprogramm ″IBM FFE″ unterstützt nicht das Ausführen von Anwendungen von einem geschützten Ordner aus. Die ausführbare Datei PROGRAMM.EXE kann z. B. nicht von einem geschützten Ordner aus ausgeführt werden.

Längenbeschränkungen für Pfadnamen

Wenn Sie versuchen, einen Ordner mit Hilfe des Dienstprogramms ″IBM FFE″ zu schützen oder eine Datei oder einen Ordner von einem ungeschützten Ordner in einen geschützten Ordner zu verschieben, erhalten Sie möglicherweise eine Nachricht des Betriebssystems, die besagt, dass ein oder mehrere Pfadnamen zu lang sind. Wenn Sie diese Nachricht erhalten, überschreitet der Pfadname einer/eines oder mehrerer Dateien oder Ordner die maximal zulässige Zeichenlänge. Beheben Sie den Fehler, indem Sie entweder die Ordnerstruktur neu anordnen, so dass der Pfad verkürzt wird, oder indem Sie Ordner- oder Dateinamen kürzen.

Fehler beim Schützen eines Ordners

Wenn Sie versuchen, einen Ordner zu schützen, und eine Nachricht erhalten, die besagt, dass der Ordner nicht geschützt werden kann, da möglicherweise eine oder mehrere Dateien verwendet werden, überprüfen Sie Folgendes:

- Überprüfen Sie, ob eine der Dateien im Ordner derzeit verwendet wird.
- Wenn im Windows Explorer ein oder mehrere Teilordner eines Ordners, den Sie schützen möchten, angezeigt werden, stellen Sie sicher, dass der Ordner, den Sie zu schützen versuchen, hervorgehoben und aktiv ist und nicht einer der Teilordner.

Kapitel 3. Client Security verwenden

Administratoren können mit den zahlreichen Komponenten von Client Security die Sicherheitsfunktionen einrichten, die für IBM Clientbenutzer erforderlich sind. Sie können sich an den folgenden Beispielen orientieren, wenn Sie die Policies und die Konfiguration mit Client Security planen. Windows NT-Anwender können z. B. für die Anmeldung am System den UVM-Schutz einrichten; dadurch werden unberechtigte Benutzer daran gehindert, sich am IBM Client anzumelden.

Beispiel 1 - Ein Client unter Windows 2000 und ein Client unter Windows XP, beide mit Outlook Express

In diesem Beispiel ist auf einem IBM Client (Client 1) Windows 2000 und Outlook Express installiert, auf dem anderen Client (Client 2) Windows XP und Outlook Express. Für drei Benutzer ist die Konfiguration der UVM-Authentifizierung auf Client 1 erforderlich; ein Clientbenutzer benötigt eine Konfiguration der UVM-Benutzerauthentifizierung auf Client 2. Alle Clientbenutzer registrieren ihre Fingerabdrücke, so dass diese zur Authentifizierung verwendet werden können. In diesem Beispiel wird ein UVM-Sensor für Fingerabdrücke installiert. Außerdem wurde ermittelt, dass beide Clients die den UVM-Schutz für die Windows-Anmeldung erfordern. Der Administrator hat entschieden, dass die lokale UVM-Policy bearbeitet und von den einzelnen Clients verwendet werden soll.

Zum Einrichten von Client Security müssen Sie folgende Schritte ausführen:

1. Installieren Sie die Software auf Client 1 und Client 2. Weitere Informationen hierzu finden Sie im *Client Security Installationshandbuch*.
2. Installieren Sie die UVM-Sensoren für Fingerabdrücke und die zugehörige Software auf den einzelnen Clients.

   Weitere Informationen zu UVM-sensitiven Produkten finden Sie im World Wide Web unter der Adresse
   http://www.pc.ibm.com/ww/security/secdownload.html.
3. Konfigurieren Sie die Benutzerauthentifizierung mit UVM für die einzelnen Clients. Gehen Sie wie folgt vor:
   a. Fügen Sie in UVM Benutzer hinzu, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen. Da Client 1 drei Benutzer aufweist, müssen Sie das Hinzufügen von Benutzern in UVM wiederholen, bis alle Benutzer hinzugefügt sind.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Schutz für die Windows-Anmeldung.
   c. Registrieren Sie die Fingerabdrücke der Benutzer. Da in einer Policy festgelegt wird, dass drei Benutzer den Client 1 verwenden, müssen alle drei Benutzer ihre Fingerabdrücke registrieren.

      Anmerkung: Wenn Sie als Authentifizierungsbestimmung in der UVM-Policy für den Client Fingerabdrücke konfigurieren, müssen die einzelnen Benutzer ihre Fingerabdrücke registrieren.

4. Bearbeiten und speichern Sie eine lokale UVM-Policy auf jedem Client, der die Authentifizierung für Folgendes erfordert:
   - Anmeldung am Betriebssystem
   - Anfordern eines digitalen Zertifikats
   - Verwendung einer digitalen Signatur für E-Mails
5. Starten Sie die einzelnen Clients erneut, um den UVM-Schutz für die Windows-Anmeldung zu aktivieren.
6. Informieren Sie die Benutzer über die UVM-Verschlüsselungstexte, die Sie für sie konfiguriert haben, und über die Authentifizierungsbestimmungen, die Sie für den IBM Client in der UVM-Policy konfiguriert haben.

Clientbenutzer können folgende Tasks ausführen:

- Sie können den UVM-Schutz zum Sperren und Entsperren des Betriebssystems verwenden.
- Sie können ein digitales Zertifikat anfordern und den integrierten IBM Security Chip auswählen, um die zum Zertifikat gehörige Verschlüsselung bereitzustellen.
- Sie können das digitale Zertifikat zur Verschlüsselung von E-Mails verwenden, die mit Outlook Express erstellt wurden.

Beispiel 2 - Zwei IBM Clients unter Windows 2000 mit Lotus Notes und mit dem Client Security-Bildschirmschoner

In diesem Beispiel ist auf zwei IBM Clients (Client 1 und Client 2) Windows 2000 und Lotus Notes installiert. Für zwei Benutzer ist die Konfiguration der UVM-Authentifizierung auf Client 1 erforderlich; ein Clientbenutzer benötigt eine Konfiguration der UVM-Benutzerauthentifizierung auf Client 2. Beide Clientbenutzer benötigen den UVM-Schutz für die Anmeldung am System und verwenden den Client Security-Bildschirmschoner sowie den UVM-Schutz für Lotus Notes. Der Administrator legte eine UVM-Policy für ferne Clients fest, die auf Client 1 bearbeitet und anschließend auf Client 2 kopiert wird.

Zum Einrichten von Client Security müssen Sie folgende Schritte ausführen:

1. Installieren Sie die Software auf Client 1 und Client 2. Da eine UVM-Policy für ferne Clients verwendet wird, müssen Sie denselben öffentlichen Schlüssel zur Verwaltung verwenden, wenn Sie die Software auf Client 1 und auf Client 2 installieren. Weitere Informationen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.
2. Konfigurieren Sie die Benutzerauthentifizierung mit UVM für die einzelnen Clients. Gehen Sie anschließend wie folgt vor:
   a. Fügen Sie in UVM Benutzer hinzu, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen. Da Client 1 zwei Benutzer aufweist, müssen Sie das Hinzufügen von Benutzern in UVM wiederholen, bis alle zwei Benutzer hinzugefügt sind.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Schutz für die Windows-Anmeldung.
3. Aktivieren Sie den UVM-Schutz für Lotus Notes auf beiden Clients. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Schutz für Lotus Notes verwenden” auf Seite 19.

4. Bearbeiten und speichern Sie eine UVM-Policy für ferne Clients auf Client 1, und kopieren Sie diese anschließend auf Client 2. Die UVM-Policy macht eine Benutzerauthentifizierung für das Entfernen des Bildschirmschoners, für die Anmeldung bei Lotus Notes und für die Anmeldung am Betriebssystem erforderlich. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Policy für ferne Clients bearbeiten und verwenden" auf Seite 29.
5. Starten Sie die einzelnen Clients erneut, um den UVM-Schutz für die Anmeldung am System zu aktivieren.
6. Informieren Sie die Clientbenutzer über die UVM-Verschlüsselungstexte und über die Policies, die für die einzelnen Clients festgelegt wurden.

Nun können die Benutzer im *Client Security Benutzerhandbuch* die Anweisungen zu folgenden Tasks lesen:

- Aktivierung des Client Security-Bildschirmschoners
- Verwendung des UVM-Schutzes für Windows 2000

Beispiel 3 - Mehrere IBM Clients unter Windows 2000 mit Tivoli Access Manager-Verwaltung und mit Netscape als E-Mail-Programm

Die Zielgruppe für das folgende Beispiel sind Unternehmensadministratoren, die planen, Tivoli Access Manager zur Verwaltung der mit der UVM-Policy konfigurierten Authentifizierungsobjekte zu verwenden. In diesem Beispiel ist auf mehreren IBM Clients sowohl Windows 2000 als auch Netscape installiert. Auf allen Clients ist der NetSEAT-Client, eine Komponente von Tivoli Access Manager, installiert. Auf allen Clients, die einen LDAP-Server verwenden, ist der LDAP-Client installiert. Die UVM-Policy für ferne Clients wird auf allen Clients installiert. Mit der UVM-Policy kann Tivoli Access Manager ausgewählte Authentifizierungsobjekte für Clients steuern.

In diesem Beispiel ist für einen einzigen Benutzer auf jedem Client die UVM-Konfiguration der Authentifizierung erforderlich. Alle Benutzer registrieren ihre Fingerabdrücke, so dass diese zur Authentifizierung verwendet werden können. In diesem Beispiel wird ein UVM-Sensor für Fingerabdrücke installiert, und für alle Clients ist der UVM-Schutz für die Windows-Anmeldung erforderlich.

Zum Einrichten von Client Security müssen Sie folgende Schritte ausführen:

1. Installieren Sie die Komponente Client Security auf dem Tivoli Access Manager-Server. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.
2. Installieren Sie Client Security auf allen Clients. Da eine UVM-Policy für ferne Clients verwendet wird, müssen Sie denselben öffentlichen Schlüssel zur Verwaltung verwenden, wenn Sie die Software auf allen Clients installieren. Weitere Informationen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.
3. Installieren Sie die UVM-Sensoren für Fingerabdrücke und die zugehörige Software auf den einzelnen Clients. Weitere Informationen zu verfügbaren UVM-sensitiven Produkten finden Sie im World Wide Web unter der Adresse http://www.pc.ibm.com/ww/security/secdownload.html.

4. Konfigurieren Sie auf jedem Client die Benutzerauthentifizierung mit UVM. Weitere Informationen hierzu finden Sie im Abschnitt „Benutzer entfernen" auf Seite 16. Gehen Sie anschließend wie folgt vor:
   a. Fügen Sie in UVM Benutzer hinzu, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Schutz für die Windows-Anmeldung.
   c. Registrieren Sie für die einzelnen Clientbenutzer die Fingerabdrücke. Wenn auf einem IBM Client die Authentifizierung über Fingerabdrücke erforderlich ist, müssen alle Benutzer dieses Clients ihre Fingerabdrücke registrieren.
5. Geben Sie die Informationen zur Tivoli Access Manager-Konfiguration auf den einzelnen Clients an. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.
6. Bearbeiten und speichern Sie auf einem der Clients eine UVM-Policy für ferne Clients, und kopieren Sie diese anschließend auf die anderen Clients. Konfigurieren Sie die UVM-Policy so, dass Tivoli Access Manager die folgenden Authentifizierungsobjekte steuert:
   - Anmeldung am Betriebssystem
   - Anfordern eines digitalen Zertifikats
   - Verwendung einer digitalen Signatur für E-Mails

   Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Policy für ferne Clients bearbeiten und verwenden" auf Seite 29.
7. Starten Sie die einzelnen Clients erneut, um den UVM-Schutz für die Windows-Anmeldung zu aktivieren.
8. Installieren Sie das PKCS #11-Modul des integrierten IBM Security Chips auf jedem Client. Dieses Modul unterstützt die Verschlüsselung auf Clients, die über Netscape E-Mails senden und empfangen, sowie den integrierten IBM Security Chip für die Anforderung digitaler Zertifikate. Weitere Informationen hierzu finden Sie im *Client Security Installationshandbuch*.
9. Ermöglichen Sie Tivoli Access Manager die Steuerung der IBM Client Security Solutions-Objekte, die in der Verwaltungskonsole von Tivoli Access Manager angezeigt werden.
10. Informieren Sie die Clientbenutzer über die UVM-Verschlüsselungstexte, die für die einzelnen Clients festgelegt wurden.
11. Weisen Sie die Clientbenutzer an, im *Client Security Benutzerhandbuch* die Anweisungen zu folgenden Tasks zu lesen:
   - Mit dem UVM-Schutz das Betriebssystem sperren und entsperren
   - Benutzerkonfigurationsprogramm verwenden
   - Ein Digitales Zertifikat anfordern, das den integrierten IBM Security Chip verwendet, um die zum Zertifikat gehörige Verschlüsselung bereitzustellen
   - Ein Digitales Zertifikat zur Verschlüsselung von E-Mails verwenden, die mit Netscape Express erstellt wurden

Kapitel 4. Benutzer autorisieren

Folgende Informationen sind hilfreich bei der Autorisierung von Windows-Benutzern für die Verwendung von User Verification Manager (UVM).

Authentifizierung für Clientbenutzer

Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt der Computersicherheit. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheits-Policy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.

Die UVM-Sicherheits-Policy für einen IBM Client können Sie auf eine der zwei folgenden Arten verwalten:

- Lokal mit einem Policy-Editor, der sich auf dem IBM Client befindet
- Unternehmensweite Verwaltung über Tivoli Access Manager

Chiffrierschlüssel der Hardwareverschlüsselung werden erzeugt, wenn Sie den ersten Benutzer hinzufügen.

Authentifizierungselemente

Authentifizierungselemente (z. B. UVM-Verschlüsselungstexte oder Fingerabdrücke von Benutzern) werden verwendet, um Benutzer mit dem IBM Client zu autorisieren. Wenn Sie einen Benutzer für die Verwendung von UVM autorisieren, ordnen Sie dem Clientbenutzer einen UVM-Verschlüsselungstext zu. Der UVM-Verschlüsselungstext kann bis zu 256 Zeichen lang sein und ist das wichtigste Element für die UVM-Authentifizierung. Wenn Sie einen UVM-Verschlüsselungstext zuordnen, werden für diesen Clientbenutzer Chiffrierschlüssel erstellt und in einer Datei gespeichert, die vom integrierten IBM Security Chip verwaltet wird. Wenn der IBM Client eine UVM-sensitive Einheit zur Authentifizierung verwendet, z. B. Fingerabdrücke von Benutzern, muss das Authentifizierungselement auch in UVM registriert sein.

Bei der Benutzerauthentifizierung können Sie die folgenden Sicherheitseinrichtungen von Client Security auswählen:

- **UVM-Schutz für die Anmeldung am Betriebssystem:** Der UVM-Schutz stellt sicher, dass nur Benutzer, die von UVM erkannt werden, auf den Computer zugreifen können. Lesen Sie die wichtigen Informationen im Abschnitt ″UVM-Anmeldeschutz für das Betriebssystem konfigurieren″, bevor Sie den UVM-Schutz für die Anmeldung am System aktivieren.
- **Client Security-Bildschirmschoner:** Nachdem Sie einen Clientbenutzer hinzugefügt haben, kann dieser Benutzer den Client Security-Bildschirmschoner konfigurieren und verwenden. Der Client Security-Bildschirmschoner wird mit der Anzeigeoption des Betriebssystems konfiguriert.

Vor dem Autorisieren von Benutzern

Wichtig: Autorisieren Sie nur Benutzeraccounts, mit denen eine Anmeldung am Betriebssystem möglich ist. Wenn ein Benutzeraccount autorisiert wird, der *nicht* zur Anmeldung am Betriebssystem verwendet werden kann, werden bei aktivierter gesicherter UVM-Anmeldung **alle** Benutzer für das System gesperrt.

Wenn Sie einen Clientbenutzer autorisieren, bietet das Administratordienstprogramm eine Liste mit Benutzernamen an, in der Sie eine Auswahl treffen können. Die in dieser Liste aufgeführten Namen sind Benutzeraccounts, die mit dem Betriebssystem hinzugefügt wurden. Erstellen Sie mit dem Betriebssystem Benutzeraccounts und Profile für die entsprechenden Benutzer, bevor Sie in UVM Clientbenutzer hinzufügen. Client Security funktioniert in Verbindung mit den Sicherheitseinrichtungen des Betriebssystems.

Windows XP und Windows 2000:

Mit dem Programm ″Benutzer und Kennwörter″ können Sie neue Benutzeraccounts erstellen und Benutzeraccounts oder Benutzergruppen verwalten. Weitere Informationen finden Sie in der Dokumentation zum Betriebssystem.

Unter Windows XP wird das Feld **Zu autorisierende Windows-Benutzer auswählen** nicht aktualisiert, wenn Sie auf die Schaltfläche zum Erstellen eines neuen Windows-Benutzers klicken. Sie müssen das Administratordienstprogramm beenden und erneut starten, um dieses Feld zu aktualisieren.

Anmerkungen:

1. Wenn Sie mit der Betriebssystemsoftware neue Benutzer erstellen, muss das Domänenkennwort für jeden neuen Benutzer gleich sein.
2. Autorisieren Sie keinen neuen Benutzer, dessen Windows-Benutzername zuvor geändert wurde. Andernfalls verweist UVM auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt.
3. Wenn ein Benutzeraccount, der autorisiert wurde, aus dem Windows-System gelöscht wird, listet die Schnittstelle für gesicherte UVM-Anmeldung fälschlicherweise weiterhin den Account als für die Anmeldung bei Windows geeignet auf. Dieser Account *kann nicht* zur Anmeldung bei Windows verwendet werden.
4. Nachdem ein Benutzer autorisiert wurde, dürfen Sie dessen Windows-Benutzernamen nicht ändern. Andernfalls müssen Sie den neuen Benutzernamen in UVM erneut autorisieren und alle neuen Berechtigungsnachweise anfordern.

Benutzer autorisieren

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm einsetzen möchten.

Gehen Sie wie folgt vor, um Benutzer in UVM zu autorisieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.

2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.

3. Wählen Sie im Bereich ″Zu autorisierende Windows-Benutzer auswählen″ in der Liste einen Namen aus.

   Anmerkung: Die Benutzernamen in der Liste sind durch die Benutzeraccounts definiert, die im Betriebssystem oder im Netzwerk erstellt wurden.

4. Klicken Sie auf **Autorisieren**.

   Die Anzeige ″Konfiguration der Benutzerauthentifizierung″ erscheint.

5. Geben Sie den UVM-Verschlüsselungstext für den neuen Benutzer ein, und bestätigen Sie diesen. Klicken Sie dann auf **Weiter**.

   Wenn der Verschlüsselungstext nicht die Bedingungen der Sicherheits-Policy erfüllt, erscheint eine Anzeige, die darauf hinweist, dass der eingegebene Verschlüsselungstext ungültig ist. Klicken Sie in diesem Fall auf **OK** und anschließend auf **Bedingungen für Verschlüsselungstext anzeigen**, um die Parameter anzuzeigen, die ein gültiger Verschlüsselungstext erfüllen muss.

   Wenn der Verschlüsselungstext akzeptiert wird, wird eine Nachricht angezeigt, die angibt, dass die Operation erfolgreich ausgeführt wurde.

6. Klicken Sie auf **OK**, um fortzufahren.

   Die Anzeige ″Windows-Anmeldekennwort″ erscheint. Wenn die gesicherte UVM-Anmeldung aktiviert ist, muss das aktuelle Windows-Kennwort dieses Benutzers gespeichert werden, damit sich der Benutzer am System anmelden kann. In dieser Anzeige stehen dem Administrator folgende Auswahlmöglichkeiten zur Verfügung:

   - **Aktuelles Windows-Kennwort des Benutzers jetzt speichern** Um das aktuelle Windows-Kennwort des Benutzers jetzt zu speichern, geben Sie das Kennwort des Benutzers in das entsprechende Feld ein, und bestätigen Sie es. Klicken Sie dann auf **Weiter**.

     Anmerkung: Das hier eingegebene Kennwort muss mit dem aktuellen Windows-Kennwort des Benutzers übereinstimmen. Diese Einstellung hat keinen Einfluss auf das Kennwort, das im Betriebssystem gespeichert ist.

   - **Benutzer soll Windows-Kennwort später mit dem Benutzerkonfigurationsprogramm speichern.** Soll der Benutzer das Windows-Kennwort später mit dem Benutzerkonfigurationsprogramm speichern, wählen Sie den entsprechenden Radioknopf, und klicken sie auf **Weiter**.

   Es erscheint eine Nachricht, in der mitgeteilt wird, dass der Vorgang erfolgreich abgeschlossen wurde.

7. Klicken Sie auf **Fertig stellen**.

Benutzer entfernen

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm einsetzen möchten.

Gehen Sie wie folgt vor, um die Autorisierung von Benutzern in UVM aufzuheben:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.
3. Wählen Sie im Bereich ″Für die Benutzung von UVM berechtigte Windows-Benutzer″ in der Liste einen Benutzernamen aus.
4. Klicken Sie auf **Benutzer entfernen**.
   Es wird eine Warnung angezeigt, die darauf hinweist, dass die Sicherheitsdaten des ausgewählten Benutzers einschließlich aller Schlüssel, Zertifikate, registrierter Fingerabdrücke und gespeicherter Kennwörter, gelöscht werden.
5. Klicken Sie auf **Ja**, um fortzufahren.
   Es wird eine Nachricht mit der Frage angezeigt, ob die archivierten Informationen des Benutzers gelöscht werden sollen. Wenn diese Informationen gelöscht werden, kann der Benutzer auf keinem System zuvor gespeicherte Einstellungen wiederherstellen.
6. Klicken Sie auf **Ja**, um den Vorgang abzuschließen.

Neue Benutzer erstellen

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm einsetzen möchten.

Gehen Sie wie folgt vor, um neue Benutzer zu erstellen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.
   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.
3. Klicken Sie im Bereich ″Zu autorisierende Windows-Benutzer auswählen″ auf **Neuen Windows-Benutzer erstellen**.

   Die Anzeige ″Windows-Benutzeraccounts″ erscheint.
4. Klicken Sie auf **Einen neuen Account erstellen**.
5. Geben Sie in das entsprechende Feld einen Namen für den neuen Account ein. Klicken Sie anschließend auf **Weiter**.
6. Wählen Sie mit Hilfe des entsprechenden Radioknopfs einen Accounttyp aus.
7. Klicken Sie auf **Account erstellen**.
8. Kehren Sie zum Administratordienstprogramms für das IBM Sicherheits-Subsystem zurück.

   Der neue Benutzeraccount wird im Bereich ″Zu autorisierende Windows-Benutzer auswählen″ angezeigt.

Kapitel 5. Nach dem Hinzufügen von Benutzern in UVM

Nach dem Autorisieren der Benutzer können Sie zusätzliche Client Security-Funktionen ausführen, wie z. B. folgende:

- **UVM-Schutz für die Anmeldung am Betriebssystem konfigurieren:** Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Anmeldeschutz für das Betriebssystem konfigurieren".
- **Benutzerchiffrierschlüssel archivieren:** Weitere Informationen hierzu finden Sie im Abschnitt „Position des Schlüsselarchivs ändern" auf Seite 34.
- **Client Security-Bildschirmschoner konfigurieren:** Weitere Informationen hierzu finden Sie in Kapitel 8, „Anweisungen für den Clientbenutzer", auf Seite 43.
- **Fingerabdrücke von Benutzern in UVM registrieren:** Weitere Informationen hierzu finden Sie im Abschnitt „Fingerabdrücke von Benutzern in UVM registrieren" auf Seite 18.

  Wenn vor dem Hinzufügen von Benutzern in UVM ein UVM-Sensor für Fingerabdrücke installiert wurde, können Sie die Fingerabdrücke registrieren.

UVM-Anmeldeschutz für das Betriebssystem

Der UVM-Anmeldeschutz für Systeme erweitert die Kennwortfunktionen, die vom Betriebssystem bereitgestellt werden. Die UVM-Anmeldeschnittstelle ersetzt die Anmeldung am Betriebssystem, so dass immer wenn sich ein Benutzer am System anmelden möchte, das UVM-Anmeldefenster angezeigt wird.

UVM-Anmeldeschutz für das Betriebssystem konfigurieren

Lesen Sie die folgenden Informationen, bevor Sie den UVM-Anmeldeschutz für das System konfigurieren und verwenden:

- Wenn die UVM-Policy angibt, dass die Authentifizierung über Fingerabdrücke für die Anmeldung am System erforderlich ist, und wenn für den Benutzer keine Fingerabdrücke registriert sind, muss der Benutzer Fingerabdrücke registrieren, um sich anmelden zu können.

  Wenn das Windows-Kennwort des Benutzers nicht oder falsch in UVM registriert wurde, muss der Benutzer das richtige Windows-Kennwort eingeben, um sich anzumelden.
- Löschen Sie den Inhalt des integrierten IBM Security Chips nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System. Weitere Informationen hierzu finden Sie im Abschnitt "Administratorfunktionen" in Kapitel 9, „Fehlerbehebung", auf Seite 51.
- Wenn Sie im Administratordienstprogramm das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren, kehrt das System zum Windows-Anmeldungsprozess zurück, ohne die gesicherte UVM-Anmeldung zu verwenden.
- Wenn Sie die Windows-Standardanmeldung durch die gesicherte UVM-Anmeldung ersetzen und die Cisco LEAP-Funktion aktivieren, müssen Sie das Cisco Aironet Client Utility (ACU) erneut installieren.

UVM-Anmeldeschutz für das Betriebssystem konfigurieren

Gehen Sie wie folgt vor, um den UVM-Anmeldeschutz für das Betriebssystem zu konfigurieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ erscheint.
3. Wählen Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** aus.
4. Klicken Sie auf **OK**.
5. Starten Sie den Computer erneut.

Wenn der Computer erneut gestartet wird, werden Sie aufgefordert, sich anzumelden. Weitere Informationen zum UVM-Schutz finden Sie im Abschnitt „UVM-Anmeldeschutz für das Betriebssystem" auf Seite 17.

Fingerabdrücke von Benutzern in UVM registrieren

Wenn die UVM-Policy so bearbeitet wurde, dass sie die Authentifizierung über Fingerabdrücke umfasst, muss jeder Benutzer in UVM Fingerabdrücke registrieren.

Anmerkung: Windows XP unterstützt keine Digital Persona U.are.U Pro-Lesegeräte für Fingerabdrücke.

Gehen im Administratordienstprogramm wie folgt vor, um Fingerabdrücke von Benutzern in UVM zu registrieren:

1. Wählen Sie im Bereich ″Für die Benutzung von UVM berechtigte Windows-Benutzer″ in der Liste einen Benutzernamen aus.
2. Klicken Sie auf **Benutzer bearbeiten**.

   Das Fenster ″Schlüsselkonfiguration von Client Security ändern - UVM-Benutzerattribute bearbeiten″ wird angezeigt.
3. Wählen Sie das Markierungsfeld **Bei UVM-sensitiver Einheit registrieren** aus, und klicken Sie auf **Weiter**.

   Das Fenster ″Schlüsselkonfiguration von Client Security ändern - UVM-gesicherte Einheiten″ wird angezeigt.
4. Klicken Sie auf **Fingerabdruck des Benutzers registrieren**.
5. Klicken Sie im Bereich für die Hand auf **Links** oder **Rechts**.
6. Klicken Sie auf den Bereich zur Fingerauswahl, um den zu scannenden Finger auszuwählen, und klicken Sie auf **Registrierung starten**.
7. Legen Sie den Finger auf den UVM-Sensor für Fingerabdrücke, und befolgen Sie die angezeigten Anweisungen.

   Je nach Scanner müssen Sie möglicherweise den Fingerabdruck viermal scannen. Klicken Sie auf **Brechen Sie den Vorgang für diesen Finger ab**, wenn Sie die Scannerabtastung des Fingerabdrucks abbrechen möchten.
8. Geben Sie einen anderen zu registrierenden Finger an, oder klicken Sie auf **Verlassen**, um das Programm zu beenden.

UVM-Schutz für Lotus Notes verwenden

UVM bietet erweiterte Sicherheitseinrichtungen für Lotus Notes-Benutzer.

UVM-Schutz für eine Lotus Notes-Benutzer-ID aktivieren und konfigurieren

Bevor Sie den UVM-Schutz für Lotus Notes aktivieren können, muss Notes auf dem IBM Client installiert sein, eine Notes-Benutzer-ID und ein Kennwort müssen für den Benutzer festgelegt werden, und der Notes-Benutzer muss zum Verwenden von UVM autorisiert sein.

Gehen Sie wie folgt vor, um den UVM-Schutz für Lotus Notes einzurichten:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ erscheint.
3. Wählen Sie das Markierungsfeld **Lotus Notes-Unterstützung aktivieren** aus.

   Der UVM-Schutz für die Lotus Notes-Benutzer-ID ist jetzt aktiviert. Falls erforderlich, fahren Sie mit den folgenden Schritten fort, um die Policy für die Lotus Notes-Anmeldung zu konfigurieren.
4. Klicken Sie auf **Anwendungs-Policy**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ erscheint.
5. Klicken Sie auf **Policy bearbeiten**.
6. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**. Die Anzeige ″IBM UVM-Policy: Lotus Notes-Anmeldung″ erscheint.
7. Wählen Sie auf der Registerkarte ″Objektauswahl″ im Dropdown-Menü ″Aktion″ den Eintrag ″Lotus Notes-Anmeldung″ aus.
8. Wählen Sie auf der Registerkarte ″Authentifizierungselemente″ die Authentifizierungselemente aus, die für die Lotus Notes-Anmeldung erforderlich sein sollen.
9. Klicken Sie auf **Übernehmen**, um Ihre Auswahl zu speichern.

   Die Anzeige ″Privater Administratorschlüssel erforderlich″ erscheint.
10. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen des entsprechenden Ordners die Speicherposition des privaten Schlüssels an.
11. Klicken Sie auf **OK**.

    In der Anzeige ″IBM User Verification Manager: Zusammenfassung für Policy″ wird eine Zusammenfassung der Objekte angezeigt, die über die lokale Client-Policy gesteuert werden.
12. Starten Sie Lotus Notes.

    Wenn Lotus Notes gestartet wird, ist die UVM-Kennwortregistrierung beendet.

UVM-Schutz innerhalb von Lotus Notes verwenden

Bevor Sie den UVM-Schutz für Lotus Notes verwenden können, müssen Sie die Schritte im Abschnitt „UVM-Schutz innerhalb von Lotus Notes konfigurieren" befolgen.

UVM-Schutz innerhalb von Lotus Notes konfigurieren

Gehen Sie wie folgt vor, um den UVM-Schutz innerhalb von Lotus Notes zu konfigurieren:

1. Melden Sie sich bei Lotus Notes an.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
2. Geben Sie in die verfügbaren Felder das Lotus Notes-Kennwort ein, und bestätigen Sie es.

   Nun ist das Lotus Notes-Kennwort in UVM registriert.

Lotus Notes-Kennwort neu festlegen

Gehen Sie wie folgt vor, um das Lotus Notes-Kennwort neu festzulegen:

1. Melden Sie sich bei Lotus Notes an.
2. Klicken Sie in der Menüleiste von Lotus Notes auf die Optionen **Datei > Extras > Benutzer-ID**.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
3. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   Das Fenster "Benutzer-ID" wird angezeigt.
4. Klicken Sie auf **Kennwort festlegen**.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
5. Wählen Sie den Radioknopf **Eigenes Kennwort erstellen** aus.
6. Geben Sie in die verfügbaren Felder das neue Lotus Notes-Kennwort ein, und überprüfen Sie es. Klicken Sie anschließend auf **OK**.

Anmerkung: Wenn Sie das Kennwort innerhalb von Lotus Notes in einen bereits verwendeten Wert ändern, lehnt Notes die Kennwortänderung ab, teilt dies jedoch Client Security nicht mit. Folglich speichert UVM das Kennwort, das von Notes abgelehnt wurde.

Wird beim Ändern des Kennworts in Lotus Notes eine Nachricht angezeigt, die besagt, dass das Kennwort bereits zuvor verwendet wurde, müssen Sie Lotus Notes verlassen, das Benutzerkonfigurationsprogramm starten und das alte Notes-Kennwort wiederherstellen.

Wenn das Lotus Notes-Kennwort per Zufallsgenerator festgelegt wurde und Sie die Fehlernachricht erhalten, haben Sie keine Möglichkeit, das alte Kennwort festzustellen, und können daher das Kennwort nicht manuell zurücksetzen. Sie müssen von Ihrem Administrator eine neue ID-Datei anfordern oder eine früher gesicherte Kopie der ID-Datei wiederherstellen.

UVM-Schutz für eine Lotus Notes-Benutzer-ID inaktivieren

Gehen Sie wie folgt vor, um den UVM-Schutz für eine Lotus Notes-Benutzer-ID zu inaktivieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**. Nachdem Sie das Kennwort eingegeben haben, wird das Hauptfenster des Administratordienstprogramms angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ erscheint.
3. Inaktivieren Sie das Markierungsfeld **Lotus Notes-Unterstützung aktivieren**.
4. Klicken Sie auf **OK**.

   In der Anzeige ″Operationen zur Anwendungsunterstützung″ wird eine Nachricht angezeigt, die besagt, dass die Lotus Notes-Unterstützung inaktiviert ist.

UVM-Schutz für eine gewechselte Lotus Notes-Benutzer-ID konfigurieren

Gehen Sie wie folgt vor, um von einer einer Benutzer-ID mit aktiviertem UVM-Schutz zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Schutz für eine Lotus Notes-Benutzer-ID inaktivieren".
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.
4. Zur Konfiguration des UVM-Schutzes für die Benutzer-ID, zu der Sie gewechselt sind, rufen Sie das Tool zur Lotus Notes-Konfiguration auf (von Client Security bereitgestellt) und konfigurieren den UVM-Schutz. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Schutz innerhalb von Lotus Notes verwenden" auf Seite 20.

Client Security mit Netscape-Anwendungen einsetzen

Die Anweisungen in diesem Abschnitt gelten speziell für die Verwendung von Client Security im Zusammenhang mit dem Anfordern und Anwenden digitaler Zertifikate bei Anwendungen, die den Standard PKCS #11 unterstützen, insbesondere Netscape-Anwendungen.

Weitere Informationen zur Verwendung der Sicherheitseinstellungen für Netscape-Anwendungen finden Sie in der Dokumentation, die mit Netscape geliefert wird. IBM Client Security unterstützt nur Netscape Version 4.7x.

Anmerkung: Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Den Grad der Verschlüsselung durch Client Security können Sie feststellen, indem Sie auf die Schaltfläche **Chipeinstellungen** klicken.

Für Netscape-Anwendungen PKCS #11-Module des integrierten IBM Security Chips installieren

Bevor Sie ein digitales Zertifikat verwenden können, müssen Sie das PKCS #11-Modul des integrierten IBM Security Chips im Computer installieren. Da die Installation des PKCS #11-Moduls des integrierten IBM Security Chips einen UVM-Verschlüsselungstext erfordert, müssen Sie in die Sicherheits-Policy für den Computer mindestens einen Benutzer aufnehmen.

Gehen Sie wie folgt vor, um das PKCS #11-Modul des integrierten IBM Security Chips zu installieren:

1. Öffnen Sie Netscape und klicken Sie auf **Datei > Seite öffnen**.
2. Suchen Sie die Installationsdatei IBMPKCSINSTALL.HTML.

   (Falls bei der Installation das vorgeschlagene Standardverzeichnis übernommen wurde, befindet sich die Datei im Verzeichnis C:\Program Files\IBM\Security.)
3. Öffnen Sie die Installationsdatei IBMPKCSINSTALL.HTML in Netscape.

   Nach dem Öffnen der Datei in Netscape beginnt die Installationsprozedur, und das Fenster ″UVM-Verschlüsselungstext″ wird aufgerufen.
4. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   Es wird eine Nachricht mit der Frage angezeigt, ob das Sicherheitsmodul tatsächlich installiert werden soll.
5. Klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass das Modul installiert wurde.
6. Klicken Sie auf **OK**.

PKCS #11-Anmeldeschutz für Netscape-Anwendungen verwenden

Wenn für den Computer der PKCS #11-Anmeldeschutz konfiguriert ist, müssen Sie die Authentifizierungsbestimmungen bei jeder Anmeldung bei Netscape erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Integrierten IBM Security Chip zum Generieren eines digitalen Zertifikats für Netscape-Anwendungen auswählen

Bei der Erstellung des digitalen Zertifikats werden Sie aufgefordert, die Karte oder die Datenbank auszuwählen, in der Sie den Schlüssel generieren möchten. Wählen Sie **Integriertes IBM Sicherheits-Subsystem** aus.

Weitere Informationen zum Generieren von digitalen Zertifikaten und zu deren Verwendung mit Netscape finden Sie in der Dokumentation zu Netscape.

Schlüsselarchiv für Netscape-Anwendungen aktualisieren

Sichern Sie das digitale Zertifikat nach seiner Erstellung, indem Sie das Schlüsselarchiv aktualisieren. Das Schlüsselarchiv können Sie mit dem Benutzerkonfigurationsprogramm aktualisieren.

Digitales Zertifikat für Netscape-Anwendungen verwenden

Verwenden Sie zur Anzeige, zur Auswahl und zur Verwendung digitaler Zertifikate die Sicherheitseinstellungen in den Netscape-Anwendungen. Sie müssen z. B. in den Sicherheitseinstellungen für Netscape Messenger das Zertifikat auswählen, bevor Sie es für digitale Signaturen oder für die Verschlüsselung von E-Mails verwenden können. Weitere Informationen hierzu finden Sie in der Dokumentation zu Netscape.

Nach der Installation des PKCS #11-Moduls des integrierten IBM Security Chips fordert Sie UVM bei jeder Verwendung des digitalen Zertifikats auf, die Authentifizierungsbestimmungen zu erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Wenn Sie die in der UVM-Policy festgelegten Authentifizierungsbestimmungen nicht erfüllen, wird eine Fehlernachricht angezeigt. Wenn Sie bei dieser Nachricht auf **OK** klicken, wird Netscape geöffnet. Sie können jedoch das vom integrierten IBM Security Chip generierte digitale Zertifikat erst verwenden, wenn Sie Netscape erneut starten und den richtigen UVM-Verschlüsselungstext, die Fingerabdrücke oder beides angeben.

Kapitel 6. Mit der UVM-Policy arbeiten

Bevor Sie die UVM-Policy für den lokalen Client bearbeiten, müssen Sie sicherstellen, dass mindestens ein Benutzer für die Verwendung von UVM autorisiert ist. Andernfalls erhalten Sie beim Öffnen der lokalen Policy-Datei mit dem Policy-Editor eine Fehlernachricht.

Nachdem Benutzer für die Verwendung von UVM autorisiert sind, müssen Sie für jeden IBM Client eine Sicherheits-Policy bearbeiten und speichern. Die von Client Security bereitgestellte Sicherheits-Policy wird als UVM-Policy bezeichnet und kombiniert die Einstellungen, die Sie im Abschnitt "Benutzer autorisieren" vorgenommen haben, mit den Einstellungen auf Clientebene.Mit der UVM-Policy können Sie die Sicherheits-Policy eines lokalen Clients steuern, oder Sie können die Policy auf ferne Clients in einem Netzwerk kopieren.

Das Administratordienstprogramm weist einen integrierten UVM-Policy-Editor auf, mit dem Sie die UVM-Policy für einen lokalen Client bearbeiten und speichern können. Tasks, die Sie am IBM Client ausführen, z. B. die Anmeldung am Betriebssystem oder das Ausblenden des Bildschirmschoners, werden als Authentifizierungsobjekte bezeichnet, und diesen Objekten müssen in der UVM-Policy Authentifizierungsbestimmungen zugeordnet sein. Sie können z. B. eine UVM-Policy definieren, in der die folgenden Anforderungen festgelegt sind:

- Jeder Benutzer muss einen UVM-Verschlüsselungstext eingeben und sich mit einem berührungslosen Ausweis (Proximity Badge) authentifizieren, um sich am Betriebssystem anmelden zu können.
- Jeder Benutzer muss jedes Mal einen UVM-Verschlüsselungstext eingeben, wenn ein digitales Zertifikat angefordert wird.

Sie können auch mit Tivoli Access Manager einzelne Authentifizierungsobjekte so steuern, wie diese in der UVM-Policy festgelegt sind.

In der UVM-Policy sind die Anforderungen für Authentifizierungsobjekte für den IBM Client, jedoch nicht für die einzelnen Benutzer festgelegt. Wenn Sie also in der UVM-Policy festlegen, dass für ein Objekt (z. B. für eine Anmeldung am Betriebssystem) eine Authentifizierung über Fingerabdrücke erforderlich ist, muss sich jeder Benutzer, der für die Verwendung von UVM autorisiert wird, mit einem Fingerabdruck registrieren, um dieses Objekt verwenden zu können. Weitere Informationen zum Autorisieren eines Benutzers finden Sie im Abschnitt „Benutzer entfernen" auf Seite 16.

Die UVM-Policy wird in einer Datei mit dem Namen `globalpolicy.gvm` gespeichert. Zur Verwendung von UVM auf fernen Clients muss die UVM-Policy auf einem IBM Client gespeichert sein und anschließend auf ferne Clients kopiert werden. Durch Kopieren der UVM-Policy-Datei auf ferne Clients sparen Sie möglicherweise Zeit, wenn Sie diese UVM-Policy auf den fernen Clients konfigurieren.

Lokale UVM-Policy bearbeiten

Sie bearbeiten eine lokale UVM-Policy und verwenden diese nur auf dem Client, für den Sie sie bearbeitet haben. Wenn Sie Client Security an seiner Standardposition installiert haben, wird die lokale UVM-Policy im Pfad \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm gespeichert. Mit dem UVM-Policy-Editor können Sie eine lokale UVM-Policy bearbeiten und speichern. Nur ein Benutzer, der in UVM aufgenommen wurde, kann den UVM-Policy-Editor verwenden. Die Schnittstelle für den UVM-Policy-Editor wir im Administratordienstprogramm bereitgestellt.

Wenn Sie Änderungen an der UVM-Policy speichern, werden Sie in einer Nachricht zur Eingabe des privaten Schlüssels für Administratoren aufgefordert. Geben Sie den privaten Schlüssel für Administratoren ein, und klicken Sie auf **OK**, um die Änderungen zu speichern. Wenn Sie einen falschen privaten Schlüssel für Administratoren eingeben, werden die Änderungen nicht gespeichert.

Die Authentifizierung richtet sich nach Ihrer Auswahl im Policy-Editor. Wenn Sie z. B. die Option "Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich" für die Lotus Notes-Anmeldung auswählen, werden Sie bei jeder Anmeldung bei Lotus Notes zur UVM-Authentifizierung aufgefordert. Solange Sie danach den Computer nicht warmstarten oder sich vom Computer abmelden, müssen Sie anschließend zum erneuten Zugriff auf Lotus Notes keinen Verschlüsselungstext eingeben.

Wenn Sie in der UVM-Policy festlegen, dass für ein Authentifizierungsobjekt (z. B. für eine Anmeldung am Betriebssystem) Fingerabdrücke erforderlich sind, muss jeder Benutzer, der in UVM aufgenommen wird, sich mit einem Fingerabdruck registrieren, um dieses Objekt verwenden zu können.

Beim Bearbeiten einer UVM-Policy können Sie die Zusammenfassungsinformationen der Policy anzeigen, indem Sie auf die Option ″Zusammenfassung für Policy″ klicken. Darüber hinaus können Sie mit **Übernehmen** Ihre Änderungen speichern. Wenn Sie auf **Übernehmen** klicken, werden Sie in einer Nachricht aufgefordert, den privaten Schlüssel für Administratoren einzugeben. Geben Sie den privaten Schlüssel für Administratoren ein, und klicken Sie auf **OK**, um die Änderungen zu speichern. Wenn Sie einen falschen privaten Schlüssel für Administratoren eingeben, werden die Änderungen nicht gespeichert.

Objektauswahl

Mit Hilfe von UVM-Policy-Objekten können Sie für verschiedene Benutzeraktionen unterschiedliche Sicherheitspolicies aktivieren. Gültige Objekte sind auf der Registerkarte **Objektauswahl** der Anzeige ″IBM UVM-Policy″ im Administratordienstprogramm angegeben.

Es gibt folgende gültige UVM-Policy-Objekte:

Systemanmeldung
: Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Anmelden am System erforderlich ist.

Entsperren des Systems
: Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Ausblenden des Client Security-Bildschirmschoners erforderlich ist.

Lotus Notes-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Anmelden bei Lotus Notes erforderlich ist.

Anmeldekennwort für Lotus Notes
Mit diesem Objekt wird die Authentifizierung gesteuert, die für UVM zum Generieren eines per Zufallsgenerator festgelegten Lotus Notes-Kennworts erforderlich ist.

Digitale Signatur (E-Mail)
Mit diesem Objekt wird die Authentifizierung gesteuert, die beim Klicken auf die Schaltfläche zum Signieren in Microsoft Outlook oder in Outlook Express erforderlich ist.

Entschlüsselung (E-Mail)
Mit diesem Objekt wird die Authentifizierung gesteuert, die beim Klicken auf die Schaltfläche zum Entschlüsseln in Microsoft Outlook oder in Outlook Express erforderlich ist.

Schutz für Dateien und Ordner
Mit diesem Objekt wird die Authentifizierung gesteuert, die nach der Auswahl der Ver- und Entschlüsselung über die rechte Maustaste erforderlich ist.

Password Manager
Dieses Objekt steuert die Authentifizierungsbestimmungen zum Verwenden des Programms ″IBM Password Manager″, das auf der IBM Website erhältlich ist. Wenn es aktiviert ist, sollten die meisten Benutzer die Einstellung ″Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich″ beibehalten.

Netscape - PKCS #11-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die erforderlich ist, wenn vom PKCS #11-Modul der Aufruf ″PKCS#11 C_OpenSession″ empfangen wird. Die meisten Benutzer sollten die Einstellung "Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich" beibehalten.

Entrust-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die erforderlich ist, wenn Entrust den Aufruf ″PKCS#11 C_OpenSession″ ausgibt, der vom PKCS #11-Modul empfangen werden soll. Die meisten Benutzer sollten die Einstellung "Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich" beibehalten.

Entrust-Anmeldekennwort ändern
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Ändern des Entrust-Anmeldekennworts erforderlich ist. Dazu gibt Entrust den Aufruf ″PKCS#11 C_OpenSession″ aus, der vom PKCS #11-Modul empfangen werden soll. Die meisten Benutzer sollten die Einstellung "Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich" beibehalten.

Authentifizierungselemente

Über die UVM-Policy wird festgelegt, welche verfügbaren Authentifizierungselemente für jedes aktivierte Objekte erforderlich sind. Auf diese Weise können Sie für verschiedene Benutzeraktionen unterschiedliche Sicherheits-Policies einrichten.

Auf der Registerkarte **Authentifizierungselemente** der Anzeige ″IBM UVM-Policy″ im Administratordienstprogramm können folgende Authentifizierungselemente ausgewählt werden:

Auswahl von Verschlüsselungstext
: Über diese Auswahl kann ein Administrator den UVM-Verschlüsselungstext zur Authentifizierung eines Benutzers auf eine der drei folgenden Arten festlegen:
  - Es ist immer ein neuer Verschlüsselungstext erforderlich.
  - Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich.
  - Kein Verschlüsselungstext erforderlich, wenn Bereitstellung bei der Anmeldung am System erfolgt ist.

Fingerabdruck-Auswahl
: Über diese Auswahl kann ein Administrator die Verwendung eines gescanntes Fingerabdrucks zur Authentifizierung eines Benutzers auf eine der drei folgenden Arten festlegen:
  - Es ist immer ein neuer Fingerabdruck erforderlich.
  - Nach erstem Gebrauch auf diese Weise ist kein Fingerabdruck erforderlich.
  - Kein Fingerabdruck erforderlich, wenn Bereitstellung bei der Anmeldung am System erfolgt ist.

Globale Einstellungen für Fingerabdrücke
: Über diese Auswahl kann ein Administrator eine maximale Anzahl an Authentifizierungsversuchen festlegen, bis ein Benutzer vom System gesperrt wird. Über diesen Bereich kann der Administrator auch festlegen, dass der Schutz durch die Authentifizierung über Fingerabdrücke durch den UVM-Verschlüsselungstext außer Kraft gesetzt werden kann.

Smartcard-Auswahl
: Diese Auswahl ermöglicht es einem Administrator, eine Smartcard als zusätzliche erforderliche Authentifizierungseinheit festzulegen.

Globale Smartcard-Einstellungen
: Diese Auswahl ermöglicht es einem Administrator, die Policy so festzulegen, dass Überschreibungen zugelassen werden, wenn der UVM-Verschlüsselungstext angegeben wird.

UVM-Policy-Editor verwenden

Führen Sie im Administratordienstprogramm die folgenden Schritte aus, um den UVM-Policy-Editor zu verwenden:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Anwendungs-Policy**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ erscheint.

3. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
4. Geben Sie Ihr Administratorkennwort ein, und klicken Sie auf **OK**.

   Die Anzeige ″IBM UVM-Policy″ erscheint.
5. Klicken Sie auf der Registerkarte ″Objektauswahl″ auf **Aktion** oder **Objekttyp**, und wählen Sie das Objekt aus, dem Authentifizierungsbestimmungen zugeordnet werden sollen.

   Zu den möglichen Aktionen gehören die Anmeldung am System, das Entsperren des Systems und die E-Mail-Entschlüsselung; ein Objekttyp ist z. B. ″Digitales Zertifikat anfordern″.
6. Führen Sie für jedes Objekt, das Sie auswählen, einen der folgenden Schritte aus:
   - Klicken Sie auf die Registerkarte **Authentifizierungselemente**, und bearbeiten Sie die Einstellungen für die verfügbaren Authentifizierungselemente, die Sie dem Objekt zuordnen möchten.
   - Zur Steuerung des ausgewählten Objekts über Tivoli Access Manager wählen Sie **Access Manager steuert ausgewähltes Objekt** aus. Wählen Sie diese Option nur aus, wenn Sie Tivoli Access Manager zum Steuern der Authentifizierungselemente für den IBM Client verwenden möchten. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

     Wichtig: Wenn Sie Tivoli Access Manager zur Steuerung eines Objektes auswählen, übergeben Sie die Steuerung dem Tivoli Access Manager-Objektbereich. Wenn Sie dies tun und Sie die lokale Steuerung für dieses Objekt wiederherstellen möchten, müssen Sie Client Security erneut installieren.
   - Wählen Sie **Keinen Zugriff auf ausgewähltes Objekt zulassen** aus, um den Zugriff für das von Ihnen ausgewählte Objekt zu verweigern.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Programm zu verlassen.

UVM-Policy für ferne Clients bearbeiten und verwenden

Die UVM-Policy können Sie auf mehreren IBM Clients verwenden, indem Sie die UVM-Policy für einen fernen Client bearbeiten und speichern und anschließend die UVM-Policy-Datei auf andere IBM Clients kopieren. Wenn Sie Client Security an seiner Standardposition installieren, wird die UVM-Policy-Datei im Pfad \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm gespeichert.

Kopieren Sie die folgenden Dateien auf andere ferne IBM Clients, die diese UVM-Policy verwenden:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Wenn Sie Client Security an seiner Standardposition installiert haben, lautet das Stammverzeichnis für den oben genannten Pfad \Program Files. Kopieren Sie beide Dateien in das Verzeichnis \IBM\Security\UVM_Policy\ auf den fernen Clients.

Kapitel 7. Weitere Funktionen des Sicherheitsadministrators

Wenn Sie Client Security auf IBM Clients konfigurieren, verwenden Sie das Administratordienstprogramm, um den integrierten IBM Security Chip zu aktivieren, ein Kennwort für den IBM Security Chip festzulegen, Hardwareschlüssel zu generieren und die Sicherheits-Policy festzulegen. In diesem Abschnitt erhalten Sie Anweisungen zur Verwendung weiterer Funktionen des Administratordienstprogramms.

Gehen Sie wie folgt vor, um das Administratordienstprogramm zu öffnen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Da der Zugriff auf das Administratordienstprogramm mit dem Kennwort für den IBM Security Chip geschützt ist, werden Sie in einer Nachricht aufgefordert, das Kennwort für den IBM Security Chip einzugeben.
2. Geben Sie das Kennwort für den IBM Security Chip ein, und klicken Sie auf **OK**.

Administratorkonsole verwenden

Über die Administratorkonsole von Client Security kann ein Sicherheitsadministrator administratorspezifische Tasks über Remotezugriff von seinem System aus ausführen.

Die Anwendung für die Administratorkonsole (console.exe) muss vom Verzeichnis `\program files\ibm\security` installiert und ausgeführt werden.

Diese Administratorkonsole bietet einem Sicherheitsadministrator folgende Funktionen:

- **Authentifizierungselemente übergehen oder überschreiben.** Zu den Funktionen zum Übergehen und Überschreiben, die der Administrator durchführen kann, gehören die folgenden:
  - **UVM-Verschlüsselungstext übergehen.** Diese Funktion ermöglicht es dem Administrator, das Übergehen des UVM-Verschlüsselungstextes zuzulassen. Bei Verwendung dieser Funktion wird, zusammen mit einer Kennwortdatei, ein Verschlüsselungstext per Zufallsgenerator erstellt. Der Administrator schickt die Kennwortdatei an den Benutzer und übermittelt ihm dann den Verschlüsselungstext auf einem anderen Weg. So ist die Sicherheit des neuen Verschlüsselungstextes gewährleistet.
  - **Kennwort zum Überschreiben des Fingerabdrucks/der Smartcard anzeigen/ändern.** Über diese Funktion kann der Administrator die Sicherheits-Policy auch dann außer Kraft setzen, wenn das Außerkraftsetzen von Verschlüsselungstexten für Fingerabdrücke oder Smartcard nicht erlaubt ist. Dies kann erforderlich werden, wenn das Lesegerät für Fingerabdrücke defekt oder die Smartcard nicht verfügbar ist. Der Administrator kann das Ersatzkennwort dem Benutzer mündlich mitteilen oder per E-Mail senden.

- **Auf Archivschlüsselinformationen zugreifen.** Der Administrator kann hier auf die folgenden Informationen zugreifen:
  - **Archivverzeichnis.** In diesem Feld kann der Administrator Archivschlüsselinformationen von einem fernen Standort aus suchen.
  - **Position des privaten Administratorschlüssels.** In diesem Feld kann der Administrator den privaten Administratorschlüssel suchen.
- **Andere Administratorfunktionen, die von einem fernen Standort aus durchgeführt werden können.** Über die Administratorkonsole kann der Sicherheitsadministrator von einem fernen Standort aus die folgenden Funktionen ausführen:
  - **Administratorenkonfigurationsdatei generieren.** Über diese Funktion kann der Administrator die Administratorkonfigurationsdatei generieren. Diese Datei wird benötigt, wenn ein Benutzer seinen Eintrag mit Hilfe des Clientdienstprogramms registrieren oder zurücksetzen möchte. Diese Datei wird vom Administrator in der Regel per E-Mail an den Benutzer gesendet.
  - **Konfigurationsdatei für Installationsprogramm verschlüsseln/entschlüsseln.** Diese Funktion aktiviert die Verschlüsselung der Konfigurationsdatei für das Installationsprogramm und bietet so zusätzliche Sicherheit. Mit dieser Funktion kann die Datei auch zur Bearbeitung entschlüsselt werden.
  - **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren.** Durch diese Funktion wird dieses System als CSS-Roaming-Server registriert. Nach der Registrierung können alle von UVM autorisierten Benutzer im Netzwerk auf ihre persönlichen Daten (Verschlüsselungstexte, Zertifikat, usw.) auf diesem System zugreifen.

Client in einem Netzwerk mit standortunabhängigen Zugriff mit Berechtigungsnachweis registrieren

Gehen Sie wie folgt vor, um einen Client ohne Benutzerunterstützung in einem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis zu registrieren:

1. Entschlüsseln Sie über das Konsolendienstprogramm die zuvor generierte Datei CSEC.INI. Diese Datei enthält das Hardwarekennwort und die Benutzer, die registriert werden sollen.
2. Fügen Sie im Abschnitt ″csssetup″ der Datei die Zeichenfolge `"enableroaming=1"` hinzu. Dies bedeutet, dass das System als Client für den standortunabhängigen Zugriff registriert werden soll.
3. Fügen Sie im selben Abschnitt den Eintrag `"username=OPTION"` hinzu. Für diesen Wert gibt es drei Optionen:
   a. **Die Zeichenfolge `"[promptcurrent]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn eine .dat-Datei für den derzeit angemeldeten Benutzer auf dem Roaming-Server generiert wurde und der derzeitige Benutzer das Systemregistrierungskennwort kennt. Durch diese Option wird ein Dialogfenster angezeigt, in dem der Benutzer zur Eingabe von `sysregpwd` (Systemregistrierungskennwort) aufgefordert wird. Wenn es sich um eine Installation ohne Benutzerunterstützung handeln soll, ist dem Administrator natürlich daran gelegen, dies zu vermeiden, da hierfür ein derzeit aktiver Benutzer erforderlich ist.
   b. **Die Zeichenfolge `"[current]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn für den derzeit angemeldeten Benutzer auf dem Server eine .dat-Datei generiert wurde. Das Systemregistrierungskennwort (`sysregpwd`) wird wie unter dem nächsten Punkt beschrieben behandelt.

c. **Ein tatsächlicher Benutzername, wie z. B. "joseph".** Wenn ein solcher designierter Benutzername verwendet wird, muss die Datei "joseph.dat" zuvor durch den Roaming-Server generiert worden sein. Das Systemregistrierungskennwort (sysregpwd) wird in diesem Fall wie unter dem nächsten Punkt beschrieben behandelt.

4. Wenn die Option 2 oder 3 verwendet wird, muss ein weiterer Eintrag "sysregpwd=SYSREGPW" hinzugefügt werden. Hierbei handelt es sich um das 8-stellige Kennwort für den derzeitigen Benutzer (wenn Option 2 implementiert wird) oder für den designierten Benutzer (wenn Option 3 implementiert wird).
5. Um die Clientregistrierung abzuschließen, verbinden Sie das System über den Roaming-Server mit der Archivpositionskonfiguration. Diese Archivposition wird in der Datei CSEC.INI benannt.

Beispiele für die Datei CSEC.INI

In den folgenden Beispielen werden eine CSEC.INI-Datei und deren Veränderung, je nachdem, welche Option für standortunabhängigen Berechtigungsnachweis ausgewählt wird, gezeigt. Es gibt folgende Optionen:

- **Keine Werte für standortunabhängigen Zugriff.** Diese Basisdatei ist nicht für standortunabhängigen Zugriff mit Berechtigungsnachweis aktiviert.
- **Option 1 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 1 für die Clientregistrierung aktiviert. Der derzeitige Benutzer muss das Systemregistrierungskennwort angeben.
- **Option 2 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 2 für die Clientregistrierung aktiviert. Der derzeitige Benutzer muss seine Benutzer-ID und das Systemregistrierungskennwort angeben.
- **Option 3 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 3 für die Clientregistrierung aktiviert. Der Benutzer ist designiert. Der designierte Benutzer muss das Systemregistrierungskennwort angeben.

Im Folgenden finden Sie Beispiele für vier verschiedene CSEC.INI-Dateien:

[CSSSetup]	[CSSSetup]	[CSSSetup]	[CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\jgk	kpl=c:\jgk	kpl=c:\jgk
kal=c:\jgk\archive	kal=c:\jgk\archive	kal=c:\jgk\archive	kal=c:\jgk\archive
clean=0	**enableroaming=1**	**enableroaming=1**	**enableroaming=1**
	username=	**username=[current]**	**username=joseph**
	[promptcurrent]		
	clean=0	**sysregpwd=12345678**	**sysregpwd=12345678**
		clean=0	clean=0
[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=
user1domain=0	user1domain=0	user1domain=0	user1domain=0
user1ppchange=0	user1ppchange=0	user1ppchange=0	user1ppchange=0
user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0
user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184

enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]
uvmlogon=0	uvmlogon=0	uvmlogon=0	uvmlogon=0
entrust=0	entrust=0	entrust=0	entrust=0
notes=0	notes=0	notes=0	notes=0
netscape=0	netscape=0	netscape=0	netscape=0
passman=0	passman=0	passman=0	passman=0
folderprotect=0	folderprotect=0	folderprotect=0	folderprotect=0
autoprotect=0	autoprotect=0	autoprotect=0	autoprotect=0

Position des Schlüsselarchivs ändern

Wenn das Schlüsselarchiv zum ersten Mal erstellt wird, werden von allen Chiffrierschlüsseln Kopien erstellt und an der Position gespeichert, die bei der Installation angegeben wurde.

Anmerkung: Darüber hinaus kann der Clientbenutzer die Position des Schlüsselarchivs mit dem Benutzerkonfigurationsprogramm ändern. Weitere Informationen hierzu finden Sie in Kapitel 8, „Anweisungen für den Clientbenutzer", auf Seite 43.

Gehen Sie im Administratordienstprogramm wie folgt vor, um die Position des Schlüsselarchivs zu ändern:

1. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Schlüssel konfigurieren″ erscheint.
2. Klicken Sie auf den Radioknopf **Archivposition ändern** und anschließend auf **Weiter**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Neue Position des Schlüsselarchivs″ erscheint.
3. Geben Sie den neuen Pfad ein, oder klicken Sie auf **Durchsuchen**, um den Pfad auszuwählen.
4. Klicken Sie auf **OK**.

   Es erscheint eine Nachricht, die anzeigt, dass der Vorgang beendet wurde.
5. Klicken Sie auf **Fertig stellen**.

Archivschlüsselpaar ändern

Nach der ersten Erstellung des Archivschlüsselpaars wird dieses gewöhnlich auf einer Diskette oder in einem Netzwerkverzeichnis gespeichert. Falls das Archivschlüsselpaar beschädigt wird, können Sie es durch ein anderes Archivschlüsselpaar ersetzen.

Anmerkung: Aktualisieren Sie das Archiv unbedingt, bevor Sie das Archivschlüsselpaar ändern.

Gehen Sie im Administratordienstprogramm wie folgt vor, um die das Archivschlüsselpaar zu ändern:

1. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Schlüssel konfigurieren″ erscheint.
2. Klicken Sie auf den Radioknopf **Archivschlüsselpaar für das IBM Sicherheits-Subsystems ändern** und anschließend auf **Weiter**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Neue Datei mit öffentlichem Schlüssel für UVM-Administrator″ erscheint.
3. Geben Sie im Bereich ″Neuer CSS-Archivschlüssel″ den Dateinamen für den neuen öffentlichen Archivschlüssel in das Feld ″Datei mit öffentlichem Schlüssel″ ein. Durch Klicken auf **Durchsuchen** können Sie die neue Datei suchen, oder Sie können durch Klicken auf **Erstellen** einen neuen öffentlichen Archivschlüssel generieren.

   Anmerkung: Achten Sie darauf, dass Sie den neuen öffentlichen Schlüssel an einer anderen Position als die alten Archivschlüsseldateien erstellen.
4. Geben Sie im Bereich ″Neuer CSS-Archivschlüssel″ den Dateinamen für den neuen privaten Archivschlüssel in das Feld ″Datei mit privatem Schlüssel″ ein. Durch Klicken auf **Durchsuchen** können Sie die neue Datei suchen, oder Sie können durch Klicken auf **Erstellen** ein neues Archivschlüsselpaar generieren.

   Anmerkung: Achten Sie darauf, dass Sie das neue Schlüsselpaar an einer anderen Position als die alten Archivschlüsseldateien erstellen.
5. Geben Sie im Bereich ″Alter CSS-Archivschlüssel″ den Dateinamen für den alten öffentlichen Archivschlüssel in das Feld ″Datei mit öffentlichem Schlüssel″ ein, oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
6. Geben Sie im Bereich ″Alter CSS-Archivschlüssel″ den Dateinamen für den alten privaten Archivschlüssel in das Feld ″Datei mit privatem Schlüssel″ ein, oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
7. Geben Sie in das Feld ″Archivposition″ den Pfad ein, in dem das Schlüsselarchiv gespeichert ist, oder klicken Sie auf **Durchsuchen**, um den Pfad auszuwählen.
8. Klicken Sie auf **Weiter**.

   Anmerkung: Wenn das Archivschlüsselpaar in mehrere Dateien aufgeteilt wurde, werden Sie in einer Nachricht aufgefordert, die Position und den Namen der einzelnen Dateien einzugeben. Klicken Sie, nachdem Sie die einzelnen Dateinamen in das Feld ″Schlüsseldatei″ eingegeben haben, auf die Option **Weiter lesen**.

   Es erscheint eine Nachricht, die anzeigt, dass der Vorgang erfolgreich beendet wurde.
9. Klicken Sie auf **OK**.

   Es erscheint eine Nachricht, die anzeigt, dass der Vorgang beendet wurde.
10. Klicken Sie auf **Fertig stellen**.

Schlüssel aus dem Archiv wiederherstellen

Falls Sie eine Systemplatine oder ein ausgefallenes Festplattenlaufwerk ausgetauscht haben, müssen Sie die Schlüssel möglicherweise wiederherstellen. Bei der Wiederherstellung von Schlüsseln kopieren Sie die neuesten Schlüsseldateien für Benutzer aus dem Schlüsselarchiv und speichern diese auf dem integrierten IBM Security Chip. Diese kopierten Schlüsseldateien für Benutzer befinden sich in dem Verzeichnis, in dem sie zuvor auf dem Computer gespeichert wurden, z. B. in einem Netzwerkverzeichnis oder auf einer Diskette.

Wenn infolge eines Festplattenausfalls die Integrität der Benutzerschlüssel beschädigt ist, können Sie die Schlüssel aus dem Schlüsselarchiv wiederherstellen. Beim Wiederherstellen der Schlüssel werden alle gespeicherten Schlüssel überschrieben.

Wenn Sie die Systemplatine des Computers durch eine Systemplatine mit einem integrierten IBM Security Chip ersetzen und die Chiffrierschlüssel auf dem Festplattenlaufwerk weiterhin gültig bleiben, können Sie die Chiffrierschlüssel wiederherstellen, die zuvor dem Computer zugeordnet waren, indem Sie diese mit dem integrierten IBM Security Chip auf der neuen Systemplatine erneut verschlüsseln.

Nachdem Sie den neuen Chip aktiviert und ein Kennwort für den IBM Security Chip festgelegt haben, können Sie einen Schlüssel wiederherstellen. Weitere Informationen hierzu finden Sie im Abschnitt „Integrierten IBM Security Chip aktivieren und Kennwort für den IBM Security Chip festlegen" auf Seite 41.

Anmerkung: Nach einer Wiederherstellung von Schlüsseln wird die UVM-Anmeldung automatisch aktiviert. Wenn Sie also für die UVM-Anmeldung die Authentifizierung über Fingerabdrücke festgelegt haben, MÜSSEN Sie die Software für Fingerabdrücke installieren, bevor Sie nach einer Wiederherstellung das System warmstarten, damit Sie nicht vom System gesperrt werden.

In den folgenden Anweisungen wird davon ausgegangen, dass das Administratordienstprogramm nicht durch einen Ausfall eines Festplattenlaufwerks beschädigt worden ist. Sollte der Ausfall des Festplattenlaufwerks zur Beschädigung der Dateien von Client Security geführt haben, müssen Sie Client Security möglicherweise erneut installieren.

Gehen Sie im Administratordienstprogramm wie folgt vor, um Chiffrierschlüssel aus einem Schlüsselarchiv wiederherzustellen:

Anmerkung: Wenn Sie das Schlüsselpaar für Administratoren nach der Wiederherstellung des Archivs ändern, wird eine Fehlernachricht angezeigt. Wenn dies eintritt, müssen Sie die Benutzer in UVM aufnehmen und anschließend neue Zertifikate anfordern.

1. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Schlüssel konfigurieren″ erscheint.
2. Klicken Sie auf den Radioknopf **Schlüssel des IBM Sicherheits-Subsystems über Archiv wiederherstellen** und anschließend auf **Weiter**.

   Die Anzeige ″Schlüsselkonfiguration von Client Security ändern - Schlüssel wiederherstellen″ erscheint.
3. Geben Sie in das Feld ″Archivverzeichnis (Pfad)″ den Pfad des Archivverzeichnisses ein, oder klicken Sie auf **Durchsuchen**, um das Verzeichnis auszuwählen.

4. Geben Sie in das Feld ″Datei mit öffentlichem CSS-Archivschlüssel″ den Pfad und den Dateinamen des öffentlichen Schlüssels für Administratoren ein, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen.
5. Geben Sie in das Feld ″Datei mit privatem CSS-Archivschlüssel″ den Pfad und den Dateinamen des privaten Schlüssels für Administratoren ein, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen.
6. Klicken Sie auf **Weiter**.

   Es erscheint eine Nachricht, in der mitgeteilt wird, dass der Vorgang erfolgreich abgeschlossen wurde.

   Anmerkung: Wenn der private Schlüssel für Administratoren in mehrere Dateien aufgeteilt wurde, werden Sie in einer Nachricht aufgefordert, die Position und den Namen der einzelnen Dateien einzugeben. Klicken Sie, nachdem Sie die einzelnen Dateinamen in das Feld ″Schlüsseldatei″ eingegeben haben, auf die Option **Weiter lesen**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Fertig stellen**.

Zähler für fehlgeschlagene Authentifizierungsversuche zurücksetzen

Gehen Sie im Administratordienstprogramm wie folgt vor, um für einen Benutzer den Zähler für fehlgeschlagene Authentifizierungsversuche zurückzusetzen:

1. Wählen Sie im Bereich ″Für die Benutzung von UVM berechtigte Windows-Benutzer″ einen Benutzer aus.
2. Klicken Sie auf **Zähler für fehlgeschlagene Versuche zurücksetzen**.

   Die Anzeige ″Zähler für fehlgeschlagene Versuche für BENUTZERNAME zurücksetzen″ erscheint.
3. Geben Sie für den ausgewählten Benutzer den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass der Vorgang erfolgreich ausgeführt wurde.
4. Klicken Sie auf **OK**.

Tivoli Access Manager-Einstellungsinformationen ändern

Die folgenden Informationen sind für Sicherheitsadministratoren vorgesehen, die Tivoli Access Manager zur Verwaltung von Authentifizierungsobjekten für die UVM-Sicherheits-Policy verwenden möchten. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

Auf die Tivoli Access Manager-Konfigurationsdatei zugreifen

Für die Konfiguration von Tivoli Access Manager auf dem IBM Client verwendet Client Security eine Konfigurationsdatei. Über diese Konfigurationsdatei wird Tivoli Access Manager mit dem Objekten verknüpft, an die die UVM-Policy die Steuerung übergibt. Gehen Sie im Administratordienstprogramm wie folgt vor, um auf die Tivoli Access Manager-Konfiguration zuzugreifen:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.

2. Geben Sie im Bereich ″Informationen zur Konfiguration von Tivoli Access Manager″ den Pfad und den Dateinamen der Konfigurationsdatei ein, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen.
3. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.
4. Fahren Sie mit der Prozedur zur Policy-Bearbeitung fort.

Lokalen Cache aktualisieren

Auf dem IBM Client wird ein lokales Replikat der von Tivoli Access Manager verwalteten Sicherheits-Policy-Informationen verwaltet. Sie können die Aktualisierungsfrequenz des lokalen Cache in Inkrementen von einem Monat oder einem Tag festlegen oder durch Klicken auf eine Schaltfläche den lokalen Cache sofort aktualisieren.

Gehen Sie im Administratordienstprogramm wie folgt vor, um den lokalen Cache einzustellen oder zu aktualisieren:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
2. Führen Sie im Bereich ″Aktualisierungsintervall für lokalen Cache″ einen der folgenden Schritte aus:
   - Klicken Sie auf **Lokalen Cache aktualisieren**, um den lokalen Cache jetzt zu aktualisieren.
   - Geben Sie zum Festlegen der Aktualisierungsfrequenz die Anzahl der Monate und Tage in die angezeigten Felder ein. Der Wert für die Monate und Tage gibt die Zeitspanne zwischen den geplanten Aktualisierungen an.

UVM-Verschlüsselungstext wiederherstellen

Ein UVM-Verschlüsselungstext wird für jeden Benutzer erstellt, der durch die Sicherheits-Policy für den IBM Client autorisiert ist. Da Verschlüsselungstexte verloren gehen, vergessen werden oder vom Clientbenutzer geändert werden können, bietet das Administratordienstprogramm dem Administrator die Möglichkeit, einen vergessenen oder verlorenen Verschlüsselungstext wiederherzustellen.

Gehen Sie im Administratordienstprogramm wie folgt vor, um einen Verschlüsselungstext wiederherzustellen:

1. Wählen Sie im Feld ″Für die Benutzung von UVM berechtigte Windows-Benutzer″ einen Benutzer aus.
2. Klicken Sie auf die Schaltfläche **Verschlüsselungstext ändern**.

   Die Anzeige ″Verschlüsselungstext ändern″ erscheint.
3. Geben Sie in das Feld ″Archivposition des IBM Sicherheits-Subsystems″ den Pfad und den Verzeichnisnamen des Schlüsselarchives ein, oder klicken Sie auf **Durchsuchen**, um das Verzeichnis auszuwählen.
4. Geben Sie im Bereich ″Archivschlüssel des IBM Sicherheits-Subsystems″ in das Feld ″Datei mit privatem Schlüssel″ den Pfad und den Verzeichnisnamen des privaten Schlüssels für Administratoren ein, oder klicken Sie auf **Durchsuchen**, um die Datei auszuwählen.
5. Geben Sie im Bereich ″Archivschlüssel des IBM Sicherheits-Subsystems″ in das Feld ″Datei mit öffentlichem Schlüssel″ den Pfad und den Verzeichnisnamen des öffentlichen Schlüssels für Administratoren ein, oder klicken Sie auf **Durchsuchen**, um die Datei auszuwählen.

6. Klicken Sie auf **OK**.

   In einer Nachricht wird der UVM-Verschlüsselungstext für den Benutzer angezeigt.

7. Klicken Sie auf **OK**.

   Wenn der private Schlüssel für Administratoren in mehrere Dateien aufgeteilt wurde, werden Sie in einer Nachricht aufgefordert, die Position und den Namen der einzelnen Dateien einzugeben. Klicken Sie, nachdem Sie die einzelnen Dateinamen in das Feld ″Datei mit privatem Schlüssel″ eingegeben haben, auf die Option **Weiter lesen**.

   Durch diese Prozedur werden per Zufallsgenerator ein temporäres Kennwort und eine Kennwortdatei generiert. Diese beiden Elemente sind für einen erneuten Zugriff auf as gesperrte System erforderlich.

8. Senden Sie die Datei an den Benutzer, und teilen Sie ihm das temporäre Kennwort auf einem anderen Weg mit.

Kennwort für den IBM Security Chip ändern

Sie müssen ein Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip für einen Client zu aktivieren. Nachdem Sie das Kennwort für den IBM Security Chip festgelegt haben, ist der Zugriff auf das Administratordienstprogramm durch dieses Kennwort geschützt. Sie können die Sicherheit erhöhen, indem Sie das Kennwort für den IBM Security Chip regelmäßig ändern. Wenn ein Kennwort längere Zeit gleich bleibt, ist es in geringerem Maße geschützt gegen unberechtigten Zugriff von außen. Halten Sie das Security Chip-Kennwort geheim, um zu verhindern, dass Benutzer ohne Autorisierung Einstellungen im Administratordienstprogramm ändern können. Weitere Informationen zu den Regeln für das Kennwort für den IBM Security Chip finden Sie in Anhang A, „Regeln für Kennwörter und Verschlüsselungstexte”, auf Seite 73.

Gehen Sie im Administratordienstprogramm wie folgt vor, um das Kennwort für den IBM Security Chip zu ändern:

1. Klicken Sie auf die Schaltfläche **Chipeinstellungen**.

   Die Anzeige ″Einstellungen für IBM Security Chip ändern″ erscheint.

2. Klicken Sie auf **Kennwort für Chip ändern**.

   Die Anzeige ″Kennwort für IBM Security Chip ändern″ erscheint.

3. Geben Sie in das Feld ″Neues Kennwort″ das neue Kennwort ein.
4. Geben Sie das Kennwort in das Feld ″Bestätigung″ erneut ein.
5. Klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass der Vorgang erfolgreich ausgeführt wurde.

   Achtung: Drücken Sie weder die Eingabetaste noch Tabulatortaste > Eingabetaste, um die Änderungen zu speichern. Andernfalls erscheint die Anzeige ″Chip inaktivieren″. Wenn das Fenster ″Chip inaktivieren″ geöffnet wird, inaktivieren Sie den Chip nicht, sondern schließen Sie das Fenster.

6. Klicken Sie auf **OK**.

Informationen zu Client Security anzeigen

Nach Klicken auf die Schaltfläche ″Chipeinstellungen″ im Administratordienstprogramm werden die folgenden Informationen zum integrierten IBM Security Chip und zu Client Security angezeigt:

- Versionsnummer der Firmware, die mit Client Security verwendet wird
- Verschlüsselungsstatus des integrierten Security Chips
- Gültigkeit der Chiffrierschlüssel für die Hardware
- Status des integrierten IBM Security Chips

Integrierten IBM Security Chip inaktivieren

Im Administratordienstprogramm gibt es eine Möglichkeit, den integrierten IBM Security Chip zu inaktivieren. Da das Kennwort für den IBM Security Chip erforderlich ist, um das Administratordienstprogramm zu starten und den Chip zu inaktivieren, müssen Sie das Kennwort für den IBM Security Chip vor unberechtigtem Zugriff schützen, damit unberechtigte Benutzer ihn nicht inaktivieren können.

Wichtig: Löschen Sie bei aktiviertem UVM-Schutz den Inhalt des integrierten IBM Security Chips nicht. Andernfalls haben Sie keinen Zugriff mehr auf das System. Den UVM-Schutz können Sie entfernen, indem Sie das Administratordienstprogramm öffnen und das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren. Sie müssen den Computer erneut starten, damit der UVM-Schutz für die Anmeldung am System inaktiviert wird.

Gehen Sie im Administratordienstprogramm wie folgt vor, um den integrierten IBM Security Chip zu inaktivieren:

1. Klicken Sie auf die Schaltfläche **Chipeinstellungen**.
2. Klicken Sie auf die Schaltfläche **Chip inaktivieren**, und befolgen Sie die angezeigten Anweisungen.
3. Wenn für den Computer erweiterte Sicherheitseinrichtungen aktiviert sind, müssen Sie möglicherweise das Administratorkennwort eingeben, das mit dem Programm ″Configuration/Setup Utility″ zum Inaktivieren des Chips festgelegt wurde.

Damit Sie den integrierten IBM Security Chip und die Chiffrierschlüssel für die Hardware nach der Inaktivierung verwenden können, müssen Sie den Chip erneut aktivieren.

Integrierten IBM Security Chip aktivieren und Kennwort für den IBM Security Chip festlegen

Wenn Sie nach der Softwareinstallation den integrierten IBM Security Chip aktivieren müssen, können Sie das Kennwort für den IBM Security Chip mit dem Administratordienstprogramm zurücksetzen und neue Chiffrierschlüssel konfigurieren.

Möglicherweise müssen Sie den integrierten IBM Security Chip aktivieren, um das Schlüsselarchiv nach einem Austausch der Systemplatine oder nach der Inaktivierung des Chips wiederherzustellen.

Gehen Sie wie folgt vor, um den Chip zu aktivieren und ein Kennwort für den IBM Security Chip festzulegen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   In einer Nachricht werden Sie aufgefordert, den integrierten IBM Security Chip für den IBM Client zu aktivieren.
2. Klicken Sie auf **Ja**.

   In einer Nachricht werden Sie aufgefordert, den Computer erneut zu starten. Sie müssen den Computer erneut starten, damit der integrierte IBM Security Chip aktiviert wird. Wenn für den Computer erweiterte Sicherheitseinrichtungen aktiviert sind, müssen Sie möglicherweise das Administratorkennwort eingeben, das mit dem Programm ″Configuration/Setup Utility″ zum Aktivieren des Chips festgelegt wurde.
3. Klicken Sie auf **OK**, um den Computer erneut zu starten.
4. Klicken Sie auf dem Windows-Desktop auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Da der Zugriff auf das Administratordienstprogramm mit dem Kennwort für den IBM Security Chip geschützt ist, werden Sie in einer Nachricht aufgefordert, das Kennwort für den IBM Security Chip einzugeben.
5. Geben Sie in das Feld ″Neues Kennwort″ ein neues Kennwort für den IBM Security Chip ein; geben Sie es in das Feld ″Bestätigung″ erneut ein.
6. Klicken Sie auf **OK**.

Unterstützung für Entrust aktivieren

Der integrierte IBM Security Chip arbeitet mit Client Security zusammen, so dass die Sicherheitseinrichtungen von Entrust erweitert werden. Wenn Sie die Unterstützung für Entrust auf einem Computer mit Client Security aktivieren, werden die Sicherheitsfunktionen von Entrust auf den IBM Security Chip übertragen.

Client Security findet automatisch die Datei ″entrust.ini″, um die Unterstützung für Entrust zu aktivieren. Wenn sich jedoch die Datei ″entrust.ini″ nicht im normalen Pfad befindet, wird ein Dialogfenster geöffnet, in dem der Benutzer nach der Datei ″entrust.ini″ suchen kann. Sobald der Benutzer die Datei gefunden und ausgewählt hat, kann Client Security die Unterstützung für Entrust aktivieren. Nach Auswahl des Markierungsfelds **Entrust-Unterstützung aktivieren** muss ein Neustart durchgeführt werden, damit Entrust den integrierten IBM Security Chip verwenden kann.

Gehen Sie wie folgt vor, um die Entrust-Unterstützung zu aktivieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
3. Wählen Sie das Markierungsfeld **Entrust-Unterstützung aktivieren** aus.
4. Klicken Sie auf **Übernehmen**.

   In der Anzeige ″Entrust-Unterstützung von IBM Client Security″ wird eine Nachricht darüber ausgegeben, dass die Entrust-Unterstützung aktiviert ist.

Anmerkung: Sie müssen den Computer erneut starten, damit die Änderungen wirksam werden.

Kapitel 8. Anweisungen für den Clientbenutzer

Hier finden Sie Informationen zu den folgenden Tätigkeiten von Clientbenutzern:

- UVM-Schutz für die Anmeldung am System verwenden
- Client Security-Bildschirmschoner konfigurieren
- Benutzerkonfigurationsprogramm verwenden
- E-Mails sicher versenden und im World Wide Web sicher navigieren
- Einstellungen für UVM-Signaltöne konfigurieren

UVM-Schutz für die Anmeldung am System verwenden

In diesem Abschnitt finden Sie Informationen zur Verwendung der gesicherten UVM-Anmeldung für die Anmeldung am System. Bevor Sie den UVM-Schutz verwenden können, muss dieser für den Computer aktiviert sein.

Mit dem UVM-Schutz können Sie den Zugriff auf das Betriebssystem über eine Anmeldeschnittstelle steuern. Die gesicherte UVM-Anmeldung ersetzt die Anmeldeanwendung von Windows, so dass sich beim Entsperren des Computers durch einen Benutzer statt des Windows-Anmeldefensters das UVM-Anmeldefenster öffnet. Wenn der UVM-Schutz für den Computer aktiviert ist, wird die UVM-Anmeldeschnittstelle beim Start des Computers aufgerufen.

Während das System aktiv ist, können Sie die UVM-Anmeldeschnittstelle mit der Tastenkombination **Strg+Alt+Entf** aufrufen, um damit den Computer herunterzufahren, zu sperren, den Task-Manager zu öffnen oder den aktuellen Benutzer abzumelden.

Client entsperren

Einen Windows-Client mit aktiviertem UVM-Schutz können Sie folgendermaßen entsperren:

1. Drücken Sie die Tastenkombination **Strg+Alt+Entf**, um auf die UVM-Anmeldeschnittstelle zuzugreifen.
2. Geben Sie den Benutzernamen und die Domäne ein, an der Sie angemeldet sind, und klicken Sie anschließend auf **Entsperren**.

   Das Fenster ″UVM-Verschlüsselungstext″ wird geöffnet.

   Anmerkung: Obwohl UVM mehrere Domänen erkennt, muss das Benutzerkennwort für alle Domänen übereinstimmen.
3. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**, um auf das Betriebssystem zuzugreifen.

Anmerkungen:

1. Wenn der UVM-Verschlüsselungstext für den eingegebenen Benutzernamen und für die eingegebene Domäne nicht der richtige ist, wird das UVM-Anmeldefenster erneut geöffnet.
2. Je nach den Authentifizierungsbestimmungen der UVM-Policy für den Client kann möglicherweise eine weiter reichende Authentifizierung erforderlich sein.

Client Security-Bildschirmschoner

Der Client Security-Bildschirmschoner besteht aus einer Serie sich bewegender Bilder, die angezeigt werden, wenn der Computer für eine angegebene Zeitspanne nicht benutzt wird. Wenn Sie den Client Security-Bildschirmschoner konfigurieren, können Sie den Zugriff auf den Computer über eine Bildschirmschoneranwendung steuern. Wenn der Client Security-Bildschirmschoner auf der Arbeitsoberfläche angezeigt wird, müssen Sie den UVM-Verschlüsselungstext eingeben, um auf die Arbeitsoberfläche des Systems zugreifen zu können.

Client Security-Bildschirmschoner konfigurieren

In diesem Abschnitt finden Sie Informationen zur Konfiguration des Client Security-Bildschirmschoners. Bevor Sie den Client Security-Bildschirmschoner verwenden können, muss mindestens ein Benutzer in der Sicherheits-Policy des betreffenden Computers registriert sein.

Zum Einrichten des Bildschirmschoners von Client Security müssen Sie folgende Schritte ausführen:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung**.
2. Klicken Sie doppelt auf das Symbol **Anzeige**.
3. Klicken Sie auf die Registerkarte **Bildschirmschoner**.
4. Wählen Sie im Dropdown-Menü ″Bildschirmschoner″ die Option **Client Security** aus. Zum Ändern der Zeitspanne, nach der der Bildschirmschoner angezeigt wird, klicken Sie auf **Einstellungen** und wählen Sie die gewünschte Zeitspanne aus.
5. Klicken Sie auf **OK**.

Verhalten des Client Security-Bildschirmschoners

Das Verhalten des Client Security-Bildschirmschoners hängt von den Einstellungen für das UVM-Administratordienstprogramm und für den Windows-Bildschirmschoner ab. Das System überprüft zuerst die Windows-Einstellungen und dann die Einstellungen für das UVM-Administratordienstprogramm. Daher sperrt der Bildschirmschoner nur, wenn das Markierungsfeld **Kennwortschutz** auf der Registerkarte mit den Windows-Einstellungen für den Bildschirmschoner aktiviert ist.

Wenn dieses Feld ausgewählt ist, fordert das System entweder das Windows-Kennwort oder den UVM-Verschlüsselungstext an, je nachdem ob im Administratordienstprogramm das Markierungsfeld **>Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** ausgewählt wurde. Wenn es ausgewählt wurde, fordert das System die Eingabe des UVM-Verschlüsselungstextes an. Wenn es nicht ausgewählt wurde, fordert das System das Windows-Kennwort an.

Darüber hinaus sind möglicherweise in der Sicherheits-Policy für den Computer weitere Authentifizierungsbestimmungen festgelegt; daher ist möglicherweise eine weiter reichende Authentifizierung erforderlich. Möglicherweise müssen Sie z. B. Ihre Fingerabdrücke mit den Scanner abtasten lassen, um den Computer zu entsperren.

Anmerkung: Wenn Sie den integrierten IBM Security Chip inaktivieren oder alle Benutzer aus der Sicherheits-Policy entfernen, ist der Client Security-Bildschirmschoner nicht verfügbar.

Benutzerkonfigurationsprogramm

Das Benutzerkonfigurationsprogramm ermöglicht es den Clientbenutzern, verschiedene Vorgänge zum Verwalten der Systemsicherheit auszuführen, für die keine Administratorberechtigungen erforderlich sind.

Funktionen des Benutzerkonfigurationsprogramms

Das Benutzerkonfigurationsprogramm bietet Clientbenutzern folgende Möglichkeiten:

- **Kennwörter und Archiv aktualisieren.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
  - **Den UVM-Verschlüsselungstext ändern:** Zum Erhöhen der Sicherheit können Sie den UVM-Verschlüsselungstext regelmäßig ändern.
  - **Windows-Kennwort aktualisieren:** Wenn Sie das Windows-Kennwort für einen UVM-berechtigten Clientbenutzer mit dem Benutzerverwaltungsprogramm von Windows ändern, müssen Sie das betreffende Kennwort auch über das Benutzerkonfigurationsprogramm von IBM Client Security ändern. Wenn ein Administrator das Administratordienstprogramm zum Ändern des Windows-Anmeldekennworts für einen Benutzer verwendet, werden alle zuvor für diesen Benutzer erstellten Chiffrierschlüssel gelöscht, und die zugeordneten digitalen Zertifikate werden ungültig.
  - **Lotus Notes-Kennwort zurücksetzen:** Zur Erhöhung der Sicherheit können Lotus Notes-Benutzer ihr Notes-Kennwort ändern.
  - **Das Schlüsselarchiv aktualisieren:** Wenn Sie digitale Zertifikate erstellen und von den privaten Schlüsseln, die auf dem integrierten IBM Security Chip gespeichert sind, Kopien erstellen möchten, oder wenn Sie das Schlüsselarchiv an eine andere Position versetzen möchten, aktualisieren Sie das Schlüsselarchiv.
- **Einstellungen für UVM-Signaltöne konfigurieren:** Mit dem Benutzerkonfigurationsprogramm können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
- **Benutzerkonfiguration.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
-
  - **Benutzer zurücksetzen.** Mit dieser Funktion können Sie Ihre Sicherheitskonfiguration wiederherstellen. Beim Zurücksetzen der Sicherheitskonfiguration werden alle Schlüssel, Zertifikate und Fingerabdrücke gelöscht.
  - **Benutzerkonfiguration über Archiv wiederherstellen:** Mit dieser Funktion können Sie Einstellungen über das Archiv wiederherstellen. Dies ist nützlich, wenn Dateien beschädigt wurden oder Sie eine vorherige Konfiguration wiederherstellen möchten.
  - **Bein einem CSS-Roaming-Server registrieren.** Mit Hilfe dieser Funktion können Sie dieses System bei einem CSS-Roaming-Server registrieren. Wenn das System registriert ist, können Sie Ihre aktuelle Konfiguration in dieses System importieren.

Einschränkungen des Benutzerkonfigurationsprogramms unter Windows XP

Unter Windows XP gibt es unter bestimmten Umständen Zugriffseinschränkungen für die für einen Clientbenutzer verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Benutzerkonfigurationsprogramm verwenden

Gehen Sie wie folgt vor, um das Benutzerkonfigurationsprogramm zu verwenden:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Hauptanzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Geben Sie für den Benutzer, dessen UVM-Verschlüsselungstext oder Windows-Kennwort geändert werden muss, den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.
3. Wählen Sie eine der folgenden Registerkarten aus:
   - **Kennwörter und Archiv aktualisieren.** Über diese Registerkarte können Sie Ihren UVM-Verschlüsselungstext ändern, Ihr Windows-Kennwort in UVM aktualisieren, Ihr Lotus Notes-Kennwort in UVM zurücksetzen und Ihr Verschlüsselungsarchiv aktualisieren.

- **UVM-Signaltöne konfigurieren.** Über diese Registerkarte können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
- **Benutzerkonfiguration.** Über diese Registerkarte kann ein Benutzer seine Benutzerkonfiguration aus dem Archiv wiederherstellen oder seine Sicherheitskonfiguration zurücksetzen.

4. Klicken Sie auf **OK**, um die Konfiguration zu beenden.

E-Mails sicher versenden und im World Wide Web sicher navigieren

Wenn Sie über das Internet ungesicherte Transaktionen senden, können diese abgefangen und gelesen werden. Den unbefugten Zugriff auf Ihre Internet-Transaktionen können Sie verhindern, indem Sie sich ein digitales Zertifikat besorgen und damit die E-Mails signieren und verschlüsseln oder den Webbrowser sichern.

Ein digitales Zertifikat (auch digitale ID oder Sicherheitszertifikat genannt) ist ein elektronischer Berechtigungsnachweis, der von einer Zertifizierungsinstanz ausgestellt und digital signiert wird. Wenn Sie ein digitales Zertifikat erhalten, bescheinigt die Zertifizierungsinstanz dadurch Ihre Identität als Eigner des Zertifikats. Bei der Zertifizierungsinstanz handelt es sich um einen vertrauenswürdigen Anbieter von digitalen Zertifikaten, z. B. eine Firma wie VeriSign oder einen Server, der als Zertifizierungsinstanz innerhalb Ihres Unternehmens eingerichtet wird. Das digitale Zertifikat enthält Ihre Identität, d. h. Ihren Namen und Ihre E-Mail-Adresse, die Ablaufdaten des Zertifikats, eine Kopie des öffentlichen Schlüssels sowie die Identität der Zertifizierungsinstanz und deren digitale Signatur.

Client Security mit Microsoft-Anwendungen einsetzen

Die nachfolgenden Informationen beziehen sich auf die Verwendung von Client Security für das Anfordern und Anwenden digitaler Zertifikate im Zusammenhang mit Anwendungen, die die Schnittstelle Microsoft CryptoAPI (z. B. Outlook Express) unterstützen.

Weitere Informationen zur Erstellung der Sicherheitseinstellungen und zur Verwendung von E-Mail-Anwendungen wie Outlook Express und Outlook finden Sie in der Dokumentation, die mit diesen Anwendungen geliefert wird.

Anmerkung: Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip die 256-Bit-Verschlüsselung unterstützen. Der Verschlüsselungsgrad von Client Security wird vom Administratordienstprogramm bestimmt.

Digitales Zertifikat für Microsoft-Anwendungen beziehen

Wenn Sie über eine Zertifizierungsinstanz ein für Microsoft-Anwendungen zu verwendendes digitales Zertifikat erstellen, werden Sie aufgefordert, für das Zertifikat einen CSP (Cryptographic Service Provider) auszuwählen.

Damit Sie die Verschlüsselungsfunktionen des integrierten IBM Security Chips für Microsoft-Anwendungen nutzen können, müssen Sie bei Erhalt des digitalen Zertifikats als CSP das **CSP-Modul des integrierten IBM Sicherheits-Subsystems** auswählen. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem IBM Security Chip gespeichert wird.

Wenn Sie die Sicherheit noch erhöhen möchten, können Sie den hohen Verschlüsselungsgrad auswählen. Da der integrierte IBM Security Chip einen Verschlüsselungsgrad von bis zu 1024 Bit für die Verschlüsselung des privaten Schlüssels des digitalen Zertifikats verarbeiten kann, sollten Sie diese Option auswählen, wenn sie von der Schnittstelle der Zertifizierungsinstanz angeboten wird; die 1024-Bit-Verschlüsselung wird hier auch als hochgradige Verschlüsselung bezeichnet.

Wenn Sie **CSP-Modul des integrierten IBM Sicherheits-Subsystems** als CSP ausgewählt haben, müssen Sie unter Umständen Ihren UVM-Verschlüsselungstext eingeben und/oder sich durch eine Sensorabtastung Ihrer Fingerabdrücke ausweisen, um die Authentifizierungsbestimmungen für das digitale Zertifikat zu erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Zertifikate vom Microsoft-CSP übertragen

Mit dem Tool zur Übertragung von Zertifikaten von Client Security können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen. Dadurch wird der notwendige Schutz für private Schlüssel, die zu Zertifikaten gehören, beträchtlich erhöht, da die Schlüssel nun statt in gefährdeter Software im integrierten IBM Security Chip sicher gespeichert sind.

Gehen Sie wie folgt vor, um das Tool zur Übertragung von Zertifikaten auszuführen:

1. Führen Sie im Stammverzeichnis der Sicherheitssoftware das Programm `xfercert.exe` aus (normalerweise in C:\Program Files\IBM\Security). Im Hauptdialogfenster werden Zertifikate angezeigt, die dem Standard-Microsoft-CSP zugeordnet sind.

   Anmerkung: Nur Zertifikate, deren private Schlüssel bei der Erstellung als *exportierbar* gekennzeichnet wurden, werden in dieser Liste angezeigt.
2. Wählen Sie die Zertifikate aus, die Sie an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen möchten.
3. Klicken Sie auf die Schaltfläche **Zertifikate übertragen**.

Die Zertifikate werden nun dem CSP-Modul des integrierten IBM Sicherheits-Subsystems zugeordnet, und die privaten Schlüssel werden vom integrierten IBM Security Chip geschützt. Alle Operationen, die diese privaten Schlüssel verwenden, z. B. die Erstellung digitaler Signaturen oder die Entschlüsselung von E-Mails, werden innerhalb der geschützten Umgebung des Chips ausgeführt.

Schlüsselarchiv für Microsoft-Anwendungen aktualisieren

Sichern Sie das digitale Zertifikat nach seiner Erstellung, indem Sie das Schlüsselarchiv aktualisieren. Sie können das Schlüsselarchiv mit dem Administratordienstprogramm aktualisieren.

Digitales Zertifikat für Microsoft-Anwendungen verwenden

Verwenden Sie zur Anzeige und zur Verwendung digitaler Zertifikate die Sicherheitseinstellungen in den Microsoft-Anwendungen. Weitere Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Nachdem Sie das digitale Zertifikat erstellt und damit eine E-Mail signiert haben, werden Sie von UVM aufgefordert, die Authentifizierungsbestimmungen beim ersten digitalen Signieren einer E-Mail zu erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen zur Verwendung des digitalen Zertifikats erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Einstellungen für UVM-Signaltöne konfigurieren

Über die Schnittstelle des Benutzerkonfigurationsprogramms können Einstellungen für Signaltöne konfiguriert werden. Gehen Sie wie folgt vor, um die Standardeinstellung für Signaltöne zu ändern:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Anzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Klicken Sie auf die Registerkarte **UVM-Signaltöne konfigurieren**.
3. Geben Sie im Abschnitt ″UVM-Authentifizierungstöne″ in das Feld ″Erfolgreiche Authentifizierung″ den Dateipfad zur Audiodatei ein, die bei erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
4. Geben Sie im Abschnitt ″UVM-Authentifizierungstöne″ in das Feld ″Authentifizierungsfehler″ den Dateipfad zur Audiodatei ein, die bei nicht erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
5. Klicken Sie auf **OK**, um den Vorgang abzuschließen.

Kapitel 9. Fehlerbehebung

Im Folgenden finden Sie Informationen zur Vermeidung, Erkennung und Behebung von Fehlern, die bei der Verwendung von Client Security auftreten können.

Administratorfunktionen

Dieser Abschnitt enthält Informationen für Administratoren zur Konfiguration und zur Verwendung von Client Security.

Administratorkennwort festlegen (ThinkCentre)

Über die Sicherheitseinstellungen im Programm ″Configuration/Setup Utility″ können Administratoren folgende Vorgänge durchführen:

- Das Hardwarekennwort für den integrierten IBM Security Chip ändern
- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Da auf Ihre Sicherheitseinstellungen über das Programm ″Configuration/Setup Utility″ des Computers zugegriffen werden kann, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″Configuration/Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″Configuration/Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **System Security** aus.
4. Wählen Sie die Option **Administrator Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
6. Geben Sie das Kennwort erneut ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.

7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie danach erneut die Eingabetaste.
8. Drücken Sie die Taste **Esc**, um die Einstellungen zu speichern und das Programm zu verlassen.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm ″Configuration/Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm ″Configuration/Setup Utility″ zugreifen und das Kennwort nicht ändern oder löschen, ohne die Computerabdeckung zu entfernen und auf der Systemplatine eine Brücke zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort festlegen (ThinkPad)

Mit den Sicherheitseinstellungen im Programm ″IBM BIOS Setup Utility″ können Administratoren folgende Vorgänge durchführen:

- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.

  Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.
- Bei einigen ThinkPad-Modellen ist es vor der Installation oder dem Upgrade von Client Security notwendig, das Administratorkennwort vorübergehend zu inaktivieren.

Nach der Konfiguration von Client Security legen Sie ein Administratorkennwort fest, um nicht berechtigte Benutzer daran zu hindern, diese Einstellungen ändern.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″IBM BIOS Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″IBM BIOS Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Password** aus.
4. Wählen Sie die Option **Supervisor Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm ″IBM BIOS Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm ″IBM BIOS Setup Utility″ zugreifen und das Kennwort nicht ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Hardwarekennwort schützen

Sie können ein Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip für einen Client zu aktivieren. Nachdem Sie das Kennwort für den IBM Security Chip festgelegt haben, ist der Zugriff auf das Administratordienstprogramm durch dieses Kennwort geschützt. Sie müssen das Kennwort für den IBM Security Chip vor unberechtigtem Zugriff schützen, damit nicht berechtigte Benutzer die Einstellungen im Administratordienstprogramm nicht ändern können.

Inhalt des integrierten IBM Security Chips löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip sowie das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter ″Achtung″ aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″Configuration/Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″Configuration/Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Taste ″Esc″, um fortzufahren.
8. Drücken Sie Taste ″Esc″, um das Programm zu verlassen und die Einstellungen zu speichern.

Inhalt des integrierten IBM Security Chips löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip und das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter ″Achtung″ aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie bei aktiviertem UVM-Schutz den integrierten IBM Security Chip nicht. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″IBM BIOS Setup Utility″ die Taste ″Fn″.

   Anmerkung: Auf einigen ThinkPad-Modellen müssen Sie möglicherweise beim Einschalten die Taste F1 drücken, um auf das Programm ″IBM BIOS Setup Utility″ zuzugreifen. Weitere Informationen hierzu finden Sie in der Hilfenachricht des Programms ″IBM BIOS Setup Utility″.

   Das Hauptmenü des Programms ″IBM BIOS Setup Utility″ wird geöffnet.
3. Wählen Sie **Config** aus.
4. Wählen Sie **IBM Security Chip** aus.
5. Wählen Sie **Clear IBM Security Chip** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Eingabetaste, um fortzufahren.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Administratordienstprogramm

Der folgende Abschnitt enthält Informationen, die Sie bei der Verwendung des Administratordienstprogramms beachten müssen.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird der Benutzername in der Benutzerliste des Administratordienstprogramms gelöscht.

Keinen Zugriff auf ausgewählte Objekte mit der Tivoli Access Manager-Steuerung zulassen

Das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** ist nicht inaktiviert, wenn die Tivoli Access Manager-Steuerung ausgewählt wurde. Wenn Sie im UVM-Policy-Editor die Option **Access Manager steuert ausgewähltes Objekt** auswählen, um ein Authentifizierungsobjekt über Tivoli Access Manager zu steuern, wird das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** nicht inaktiviert. Auch wenn das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** weiterhin aktiviert ist, kann die Tivoli Access Manager-Steuerung nicht über dieses Markierungsfeld außer Kraft gesetzt werden.

Bekannte Einschränkungen

Dieser Abschnitt enthält Informationen zu bekannten Einschränkungen in Bezug auf Client Security.

Client Security mit Windows-Betriebssystemen einsetzen

Alle Windows-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Wenn ein in UVM registrierter Clientbenutzer seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss den neuen Benutzernamen erneut in UVM registrieren und alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: In UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, werden von UVM nicht erkannt. UVM verweist auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.

Client Security mit Netscape-Anwendungen einsetzen

Netscape wird nach einem Berechtigungsfehler geöffnet: Wenn das Fenster ″UVM-Verschlüsselungstext″ geöffnet wird, müssen Sie den UVM-Verschlüsselungstext eingeben und auf **OK** klicken, bevor Sie fortfahren können. Wenn Sie einen falschen UVM-Verschlüsselungstext eingeben (oder bei einer Scanner-abtastung von Fingerabdrücken einen falschen Fingerabdruck liefern), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte digitale Zertifikat nicht verwenden. Sie müssen Netscape verlassen, erneut aufrufen und den richtigen UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat für den integrierten IBM Security Chip verwenden können.

Algorithmen werden nicht angezeigt: Beim Anzeigen des Moduls in Netscape ist keiner der vom PKCS #11-Modul des integrierten IBM Security Chips unterstützten Hashverfahren-Algorithmen ausgewählt. Die folgenden Algorithmen werden vom PKCS #11-Modul des integrierten IBM Security Chips unterstützt, jedoch nicht als unterstützt erkannt, wenn sie in Netscape angezeigt werden:

- SHA-1
- MD5

Zertifikat des integrierten IBM Security Chips und Verschlüsselungsalgorithmen

Im Folgenden finden Sie Informationen zu Verschlüsselungsalgorithmen, die Sie mit dem Zertifikat des integrierten IBM Security Chips verwenden können. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Senden von E-Mails von einem Outlook Express-Client (128 Bit) an einen anderen Outlook Express-Client (128 Bit): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, um verschlüsselte E-Mails an andere Clients mit Outlook Express (128 Bit) zu senden, können mit dem Zertifikat des integrierten IBM Security Chips verschlüsselte E-Mails nur mit dem 3DES-Algorithmus verschlüsselt werden.

Beim Senden von E-Mails zwischen einem Outlook Express-Client (128 Bit) und einem Netscape-Client: Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet.

Möglicherweise stehen einige Algorithmen im Outlook Express-Client (128 Bit) nicht zur Auswahl: Je nachdem, wie die Version von Outlook Express (128 Bit) konfiguriert oder aktualisiert wurde, sind möglicherweise einige RC2-Algorithmen und andere Algorithmen für die Verwendung mit dem Zertifikat des integrierten IBM Security Chips nicht verfügbar. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

UVM-Schutz für eine Lotus Notes-Benutzer-ID verwenden

Der UVM-Schutz funktioniert nicht, wenn Sie innerhalb einer Notes-Sitzung die Benutzer-ID wechseln: Sie können den UVM-Schutz nur für die aktuelle Benutzer-ID einer Notes-Sitzung konfigurieren. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie den UVM-Schutz für die Benutzer-ID, zu der Sie gewechselt haben, konfigurieren möchten, fahren Sie mit Schritt 4 fort.
4. Rufen Sie das von Client Security bereitgestellte Tool zur Lotus Notes-Konfiguration auf, und konfigurieren Sie den UVM-Schutz.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Fehlernachrichten

Fehlernachrichten für Client Security werden in Ereignisprotokoll geschrieben: Client Security verwendet einen Einheitentreiber, der möglicherweise Fehlernachrichten in das Ereignisprotokoll schreibt. Die Fehler, auf denen diese Nachrichten basieren, wirken sich auf den normalen Betrieb des Computers nicht aus.

UVM ruft Fehlernachrichten auf, die vom zugeordneten Programm generiert werden, wenn für ein Authifizierungsobjekt der Zugriff verweigert wird: Wenn in der UVM-Policy die Verweigerung des Zugriffs für ein Authentifizierungsobjekt, z. B. für die E-Mail-Verschlüsselung festgelegt ist, variiert die Nachricht über den verweigerten Zugriff je nach verwendeter Software. Eine Fehlernachricht von Outlook Express über die Verweigerung des Zugriffs auf ein Authentifizierungsobjekt unterscheidet sich somit von einer Netscape-Fehlernachricht über verweigerten Zugriff.

Fehlerbehebungstabellen

Im folgenden Abschnitt finden Sie Tabellen, die Ihnen bei der Behebung von Fehlern in Verbindung mit Client Security weiterhelfen können.

Fehlerbehebungsinformationen zur Installation

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Installation von Client Security weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Während der Softwareinstallation wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei der Softwareinstallation werden Sie in einer Nachricht gefragt, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Beginnen Sie erneut mit dem Installationsprozess, um die neue Version von Client Security zu installieren.
Während der Installation wird eine Nachricht angezeigt, die besagt, dass bereits eine vorherige Version von Client Security installiert ist.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Gehen Sie wie folgt vor: 1. Deinstallieren Sie die Software. 2. Installieren Sie die Software erneut. **Anmerkung:** Wenn Sie dasselbe Hardwarekennwort zum Schutz des integrierten IBM Security Chips verwenden möchten, müssen Sie den Inhalt des Chips nicht löschen und kein neues Kennwort festlegen.
Der Installationszugriff wird verweigert, da das Hardwarekennwort unbekannt ist	**Maßnahme**
Wenn Sie die Software auf einem IBM Client mit aktiviertem integrierten IBM Security Chip installieren, ist das Hardwarekennwort für den integrierten IBM Security Chip unbekannt.	Löschen Sie den Inhalt des Chips, um mit der Installation fortzufahren.
Die Datei ″setup.exe″ reagiert nicht ordnungsgemäß (CSS Version 4.0x)	**Maßnahme**
Wenn Sie alle Dateien aus ″csec4_0.exe″ in ein gemeinsames Verzeichnis extrahieren, funktioniert die Datei ″setup.exe″ nicht ordnungsgemäß.	Führen Sie die Datei ″smbus.exe″ aus, um den SMBus-Einheitentreiber zu installieren, und führen Sie anschließend die Datei ″csec4_0.exe″ aus, um den Softwarecode von Client Security zu installieren.

Fehlerbehebungsinformationen zum Administratordienst-programm

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung des Administratordienstprogramms weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Policy für UVM-Verschlüsselungstext nicht erzwungen	**Maßnahme**
Das Markierungsfeld **Mehr als 2 wiederkehrende Zeichen nicht zulassen** funktioniert nicht in IBM Client Security Version 5.0	Dies ist eine bekannte Einschränkung bei IBM Client Security Version 5.0.
Die Schaltfläche "Weiter" ist nicht verfügbar, nachdem Sie im Administratordienstprogramm den UVM-Verschlüsselungstext eingegeben und bestätigt haben.	**Maßnahme**
Wenn Sie neue Benutzer in UVM aufnehmen, ist die Schaltfläche **Weiter** möglicherweise nicht mehr verfügbar, nachdem Sie Ihren UVM-Verschlüsselungstext im Administratordienstprogramm eingegeben und bestätigt haben.	Klicken Sie in der Windows-Taskleiste auf **Informationen**, und fahren Sie mit dem Vorgang fort.
Beim Versuch, eine lokale UVM-Policy zu bearbeiten, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Beim Bearbeiten der lokalen UVM-Policy wird möglicherweise eine Fehlernachricht angezeigt, wenn in UVM keine Benutzer registriert sind.	Fügen Sie in UVM einen Benutzer hinzu, bevor Sie versuchen, die Policy-Datei zu bearbeiten.
Beim Ändern des öffentlichen Schlüssels für Administratoren wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie den Inhalt des integrierten Security Chips löschen und anschließend das Schlüsselarchiv wiederherstellen, wird bei der Änderung des öffentlichen Schlüssels für Administratoren möglicherweise eine Fehlernachricht angezeigt.	Fügen Sie in UVM die Benutzer hinzu, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie einen öffentlichen Schlüssel für Administratoren ändern und anschließend versuchen, einen UVM-Verschlüsselungstext für einen Benutzer wiederherzustellen, wird möglicherweise eine Fehlernachricht angezeigt.	Führen Sie einen der folgenden Schritte aus: • Sollte für den Benutzer der UVM-Verschlüsselungstext nicht benötigt werden, ist keine Maßnahme erforderlich. • Wenn der UVM-Verschlüsselungstext für den Benutzer erforderlich ist, müssen Sie ihn in UVM aufnehmen und ggf. neue Zertifikate anfordern.

Fehlersymptom	Mögliche Lösung
Beim Versuch, die UVM-Policy-Datei zu speichern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine UVM-Policy-Datei (globalpolicy.gvm) durch Klicken auf **Übernehmen** oder **Speichern** zu speichern, wird eine Fehlernachricht angezeigt.	Schließen Sie die Fehlernachricht, bearbeiten Sie die UVM-Policy-Datei erneut, und speichern Sie die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der aktuelle Benutzer, der am Betriebssystem angemeldet ist, nicht in UVM aufgenommen wurde, wird der UVM-Policy-Editor nicht geöffnet.	Nehmen Sie den Benutzer in UVM auf, und öffnen Sie den UVM-Policy-Editor.
Bei der Verwendung des Administratordienstprogramms wird eine Fehlernachricht angezeigt.	**Maßnahme**
Während Sie das Administratordienstprogramm verwenden, wird möglicherweise die folgende Fehlernachricht angezeigt: Beim Versuch, auf den Client Security Chip zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Der Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Kennworts für den Security Chip wird eine Nachricht über die Inaktivierung des Chips angezeigt.	**Maßnahme**
Wenn Sie versuchen, das Kennwort für den IBM Security Chip zu ändern, und nach der Eingabe des Bestätigungskennworts die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste drücken, wird die Schaltfläche ″Chip inaktivieren″ aktiviert, und es wird eine Bestätigungsnachricht für das Inaktivieren des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster für die Inaktivierung des Chips. 2. Geben Sie zum Ändern des Kennworts für den IBM Security Chip das neue Kennwort ein, geben Sie das Bestätigungskennwort ein, und klicken Sie anschließend auf **Ändern**. Drücken Sie, nachdem Sie das Bestätigungskennwort eingegeben haben, nicht die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste.

Fehlerbehebungsinformationen zum Benutzerkonfigurationsprogramm

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung des Benutzerkonfigurationsprogramms Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Benutzer mit eingeschränkter Berechtigung können gewisse Funktionen des Benutzerkonfigurationsprogramms unter Windows XP Professional nicht ausführen	**Maßnahme**
Benutzer von Windows XP Professional mit eingeschränkter Berechtigung können möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen: • Den UVM-Verschlüsselungstext ändern • Das mit UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.
Benutzer mit eingeschränkter Berechtigung können das Benutzerkonfigurationsprogramm unter Windows XP Home nicht ausführen	**Maßnahme**
Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden: • Client Security ist auf einer Partition im NTFS-Format installiert. • Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format. • Der Archivordner befindet sich auf einer Partition im NTFS-Format.	Dies ist eine bekannte Einschränkung unter Windows XP Home. Für dieses Problem gibt es keine Lösung.

Fehlerbehebungsinformationen zum ThinkPad

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Client Security auf ThinkPads weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht mit folgendem Wortlaut angezeigt: ″FEHLER 0197: Ungültige ferne Änderungsanforderung. Drücken Sie <F1>, um Setup aufzurufen.″	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit Sie bestimmte Administratorfunktionen von Client Security ausführen können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Rufen Sie mit ″F1″ das Programm ″IBM BIOS Setup Utility″ auf. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie ein leeres neues Administratorkennwort ein, und bestätigen Sie das leere Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.
Ein anderer UVM-Sensor für Fingerabdrücke funktioniert nicht ordnungsgemäß.	**Maßnahme**
Der IBM ThinkPad unterstützt den Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht.	Wechseln Sie die Modelle der Sensoren für Fingerabdrücke nicht. Verwenden Sie bei der Arbeit von einem fernen Standort aus stets das gleiche Modell wie bei der Arbeit an einer Andockstation.

Fehlerbehebungsinformationen zu Microsoft-Anwendungen und -Betriebssystemen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Microsoft-Anwendungen oder -Betriebssystemen.

Fehlersymptom	Mögliche Lösung
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktop wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt wird.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Windows Media Player-Dateien werden verschlüsselt, statt unter Windows XP wiedergegeben zu werden.	**Maßnahme**

Fehlersymptom	Mögliche Lösung
Wenn Sie unter Windows XP einen Ordner öffnen und auf **Alles wiedergeben** klicken, wird der Dateiinhalt verschlüsselt, statt vom Windows Media Player wiedergegeben zu werden.	Gehen Sie wie folgt vor, um die Wiedergabe von Dateien mit dem Windows Media Player zu aktivieren: 1. Starten Sie den Windows Media Player. 2. Wählen Sie alle Dateien im entsprechenden Ordner aus. 3. Ziehen Sie die Dateien in den Bereich "Wiedergabeliste" von Windows Media Player.
Client Security funktioniert für einen in UVM registrierten Benutzer nicht ordnungsgemäß.	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. Wenn dies zutrifft, geht die gesamte Funktionalität von Client Security verloren.	Registrieren Sie den neuen Benutzernamen in UVM erneut, und fordern Sie alle neuen Berechtigungsnachweise an.
Anmerkung: Unter Windows XP werden in UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, von UVM nicht erkannt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.	
Fehler beim Lesen verschlüsselter E-Mails mit Outlook Express	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des Webbrowsers beim Sender muss mit dem Verschlüsselungsgrad des Webbrowsers des Empfängers kompatibel sein. 2. Der Verschlüsselungsgrad des Webbrowsers muss mit dem Verschlüsselungsgrad der Firmware von Client Security kompatibel sein.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, der mehrere Zertifikate zugeordnet sind	**Maßnahme**
Outlook Express kann mehrere Zertifikate zu einer einzigen E-Mail-Adresse auflisten, und einige dieser Zertifikate können ungültig werden. Ein Zertifikat wird ungültig, wenn der dem Zertifikat zugeordnete private Schlüssel auf dem integrierten IBM Security Chip des Sendercomputers, auf dem das Zertifikat generiert wurde, nicht mehr vorhanden ist.	Bitten Sie den Empfänger, sein digitales Zertifikat erneut zu senden; wählen Sie anschließend dieses Zertifikat im Adressbuch von Outlook Express aus.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der Verfasser einer E-Mail versucht, eine E-Mail digital zu signieren, jedoch seinem E-Mail-Account noch kein Zertifikat zugeordnet ist, wird eine Fehlernachricht angezeigt.	Verwenden Sie die Sicherheitseinstellungen in Outlook Express, um ein Zertifikat anzugeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128 Bit) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus.	**Maßnahme**
Beim Senden verschlüsselter E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, kann nur der 3DES-Algorithmus verwendet werden.	Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit Outlook Express verwendet werden, erhalten Sie bei Microsoft.
Outlook Express-Clients senden E-Mails mit einem anderen Algorithmus zurück.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Bei der Verwendung eines Zertifikats in Outlook Express wird nach dem Ausfall eines Festplattenlaufwerks eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Führen Sie nach der Wiederherstellung der Schlüssel einen der folgenden Schritte aus: • Fordern Sie neue Zertifikate an. • Registrieren Sie die Zertifizierungsinstanz erneut in Outlook Express.

Fehlersymptom	Mögliche Lösung
Outlook Express aktualisiert den dem Zertifikat zugeordneten Verschlüsselungsgrad nicht.	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Outlook Express-Client mit Internet Explorer 4.0 (128 Bit) sendet, stimmt möglicherweise der Verschlüsselungsgrad der zurückgesendeten E-Mail nicht überein.	Löschen Sie das zugeordnete Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und fügen Sie dem Adressbuch von Outlook Express das Zertifikat hinzu.
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können in Outlook Express eine Nachricht öffnen, indem Sie doppelt darauf klicken. Wenn Sie zu schnell auf eine verschlüsselte Nachricht klicken, wird in einigen Fällen eine Nachricht über Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Darüber hinaus wird möglicherweise in der Voranzeige eine Fehlernachricht angezeigt, wenn Sie eine verschlüsselte Nachricht auswählen.	Wenn in der Voranzeige eine Fehlernachricht angezeigt wird, ist keine Maßnahme erforderlich.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche ″Senden″ klicken, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie in Outlook Express zweimal auf die Schaltfläche zum Senden klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht darüber angezeigt, dass die Nachricht nicht gesendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie einmal auf die Schaltfläche **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei Verwendung von Internet Explorer erhalten Sie möglicherweise eine Fehlernachricht, wenn Sie ein Zertifikat anfordern, das das CSP-Modul des integrierten IBM Security Chips verwendet.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Netscape-Anwendungen.

Fehlersymptom	Mögliche Lösung
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des vom Sender verwendeten Webbrowsers ist mit dem Verschlüsselungsgrad des vom Empfänger verwendeten Webbrowsers kompatibel. 2. Der Verschlüsselungsgrad des Webbrowsers ist mit dem Verschlüsselungsgrad kompatibel, der von der Firmware von Client Security bereitgestellt wird.
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Security Chips in Netscape Messenger nicht ausgewählt wurde und der Verfasser der E-Mail versucht, diese mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Verwenden Sie zur Auswahl des Zertifikats die Sicherheitseinstellungen in Netscape Messenger. Wenn Netscape Messenger geöffnet ist, klicken Sie in der Symbolleiste auf das Sicherheitssymbol. Das Fenster mit den Sicherheitsinformationen wird geöffnet. Klicken Sie im linken Teilfenster auf **Netscape Messenger**, und wählen Sie anschließend **Zertifikat des integrierten IBM Security Chips** aus. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.
Eine E-Mail wird mit einem anderen Algorithmus an den Client zurückgesendet.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

Fehlersymptom	Mögliche Lösung
Ein digitales Zertifikat, das vom integrierten IBM Security Chip generiert wurde, kann nicht verwendet werden.	**Maßnahme**
Das vom integrierten IBM Security Chip generierte digitale Zertifikat ist nicht verfügbar.	Überprüfen Sie, ob Sie beim Öffnen von Netscape den richtigen UVM-Verschlüsselungstext eingegeben haben. Wenn Sie den falschen UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht über einen Authentifizierungsfehler angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte Zertifikat nicht verwenden. Sie müssen Netscape verlassen und erneut öffnen und anschließend den richtigen UVM-Verschlüsselungstext eingeben.
Neue digitale Zertifikate vom selben Sender werden innerhalb von Netscape nicht ausgetauscht.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals empfangen wird, wird das erste digitale Zertifikat, das der E-Mail zugeordnet ist, nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate empfangen, ist das einzige Zertifikat das Standardzertifikat. Löschen Sie mit den Sicherheitseinrichtungen in Netscape das erste Zertifikat, und öffnen Sie anschließend das zweite Zertifikat erneut, oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.
Das Zertifikat des integrierten IBM Security Chips kann nicht exportiert werden.	**Maßnahme**
Das Zertifikat des integrierten IBM Security Chips kann in Netscape nicht exportiert werden. Die Exportfunktion in Netscape können Sie zum Sichern von Zertifikaten verwenden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden von allen Zertifikaten, die dem integrierten IBM Security Chip zugeordnet sind, Kopien erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach dem Ausfall eines Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Fordern Sie nach dem Wiederherstellen der Schlüssel ein neues Zertifikat an.

Fehlersymptom	Mögliche Lösung
Der Netscape-Agent wird geöffnet und verursacht einen Fehler in Netscape.	**Maßnahme**
Das Öffnen des Netscape-Agenten führt zum Schließen von Netscape.	Schalten Sie den Netscape-Agenten aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips hinzufügen und anschließend Netscape öffnen, verzögert sich das Öffnen von Netscape um kurze Zeit.	Es ist keine Maßnahme erforderlich. Dies dient lediglich zu Ihrer Information.

Fehlerbehebungsinformationen zu digitalen Zertifikaten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Anforderung eines digitalen Zertifikats Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Das Fenster ″UVM-Verschlüsselungstext″ oder das Fenster für die Authentifizierung über Fingerabdrücke wird bei der Anforderung eines digitalen Zertifikats mehrmals angezeigt.	**Maßnahme**
In der UVM-Sicherheits-Policy ist festgelegt, dass ein Benutzer sich mit einem UVM-Verschlüsselungstext oder über Fingerabdrücke authentifizieren muss, bevor er ein digitales Zertifikat erhalten kann. Wenn der Benutzer versucht, ein Zertifikat zu erhalten, wird das Authentifizierungsfenster, in dem er aufgefordert wird, den UVM-Verschlüsselungstext anzugeben oder die Fingerabdrücke abtasten zu lassen, mehrmals angezeigt.	Geben Sie bei jedem Öffnen des Authentifizierungsfensters den UVM-Verschlüsselungstext ein bzw. lassen Sie ihre Fingerabdrücke abtasten.
Eine Nachricht über einen VBScript- oder JavaScript-Fehler wird angezeigt.	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht angezeigt, die sich auf VBScript oder JavaScript bezieht.	Starten Sie den Computer erneut, und beziehen Sie das Zertifikat erneut.

Fehlerbehebungsinformationen zu Tivoli Access Manager

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Tivoli Access Manager in Verbindung mit Client Security Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration eines PD-Servers vorgenommen hat.	Dies ist eine bekannte Einschränkung.
Kein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traversebit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Lotus Notes mit Client Security weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann Lotus Notes die Konfiguration nicht fertig stellen.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert werden und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie das Notes-Kennwort bei Verwendung von Client Security ändern, wird dies in einer Fehlernachricht angezeigt.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client neu.
Nach dem Festlegen eines Kennworts per Zufallsgenerator wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie folgende Vorgänge ausführen, wird möglicherweise eine Fehlernachricht angezeigt: • Verwenden des Tools zur Lotus Notes-Konfiguration zur Einstellung des UVM-Schutzes für eine Notes-ID • Öffnen von Notes und Verwenden der Notes-Funktion zur Kennwortänderung für die Datei mit der Notes-ID • Schließen von Notes sofort nach der Kennwortänderung	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, generiert UVM ein neues, per Zufallsgenerator festgelegtes Kennwort für die Notes-ID.

Fehlerbehebungsinformationen zur Verschlüsselung

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verschlüsselung von Dateien unter Verwendung von Client Security ab Version 3.0 weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Bereits verschlüsselte Dateien werden nicht entschlüsselt.	**Maßnahme**
Dateien, die mit früheren Versionen von Client Security verschlüsselt wurden, werden nach dem Upgrade auf Client Security ab Version 3.0 nicht entschlüsselt.	Dies ist eine bekannte Einschränkung. Sie müssen alle mit früheren Versionen von Client Security verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann Dateien, die von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung UVM-sensitiver Einheiten weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Anschluss (Universal Serial Bus) trennen und die Einheit danach erneut am USB-Anschluss anschließen, funktioniert die Einheit möglicherweise nicht ordnungsgemäß.	Starten Sie nach dem erneuten Anschluss der Einheit an den USB-Anschluss den Computer erneut.

Anhang A. Regeln für Kennwörter und Verschlüsselungstexte

In diesem Anhang finden Sie Informationen zu den Regeln für verschiedene Systemkennwörter.

Regeln für Hardwarekennwörter

Für Hardwarekennwörter gelten die folgenden Regeln:

Länge Das Kennwort muss genau acht Zeichen lang sein.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Die Kombination von Buchstaben und Ziffern ist zulässig. Es sind keine speziellen Zeichen wie das Leerzeichen und die Zeichen !, ?, % zulässig.

Merkmale
Sie können das Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort müssen Sie bei jedem Zugriff auf das Administratordienstprogramm eingeben.

Fehlversuche
Wenn Sie das Kennwort zehnmal falsch eingegebenen haben, wird der Computer 1 Stunde und 17 Minuten lang gesperrt. Wenn Sie nach diesem Zeitraum das Kennwort zehn weitere Male falsch eingeben, wird der Computer 2 Stunden und 34 Minuten lang gesperrt. Die Dauer der Computersperrung verdoppelt sich jedes Mal, wenn Sie das Kennwort zehnmal falsch eingeben.

Regeln für UVM-Verschlüsselungstexte

Die Sicherheit wird dadurch erhöht, dass der UVM-Verschlüsselungstext länger und eindeutiger ist als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm von IBM Client Security gesteuert.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung von Kriterien für Verschlüsselungstexte bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator folgende Regeln für Verschlüsselungstexte festlegen:

Anmerkung: Die Standardeinstellung für jedes Kriterium ist unten in Klammern angegeben.

- ob eine Mindestanzahl an alphanumerischen Zeichen festgelegt werden soll (ja, 6)

  Wenn z. B. der Wert ″6″ festgelegt ist, ist der Verschlüsselungstext `1234567xxx` ungültig.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn z. B. der Wert ″1″ festgelegt ist, ist der Verschlüsselungstext `thisismypassword` ungültig.

- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn z. B. der Wert ″2″ festgelegt ist, ist der Verschlüsselungstext `i am not here` ungültig.
- ob mehr als zwei wiederkehrende Zeichen zulässig sein sollen (nein)

  Wenn dies z. B. festgelegt ist, ist der Verschlüsselungstext `aaabcdefghijk` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `1password` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer enden darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password8` ungültig.
- ob der Verschlüsselungstext eine Benutzer-ID enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `Benutzername` ungültig, wobei es sich bei `Benutzername` um eine Benutzer-ID handelt.
- ob der neue Verschlüsselungstext sich von den letzten x Verschlüsselungstexten unterscheiden muss (ja, 3)

  Standardmäßig ist z. B. der Verschlüsselungstext `mypassword` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinander folgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `pass` oder `word` war.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms ermöglicht Sicherheitsadministratoren zudem eine Steuerung des Ablaufs der Verschlüsselungstexte. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator aus den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext ist nicht mehr gültig nach (ja, 184).

  In diesem Beispiel läuft der Verschlüsselungstext standardmäßig nach 184 Tagen ab. Der neue Verschlüsselungstext muss der vorhandenen Policy für den Verschlüsselungstext entsprechen.
- Verschlüsselungstext läuft nie ab.

  Wenn diese Option ausgewählt ist, läuft der Verschlüsselungstext nie ab.

Die Policy für den Verschlüsselungstext wird vom Administratordienstprogramm bei der Registrierung des Benutzers und bei der Änderung des Verschlüsselungstextes durch den Benutzer über das Clientdienstprogramm überprüft. Die beiden Benutzereinstellungen zum vorherigen Kennwort werden zurückgesetzt, und Protokolle zum Verschlüsselungstext werden entfernt.

Folgende allgemeine Regeln gelten für UVM-Verschlüsselungstexte:

Länge Der Verschlüsselungstext kann bis zu 256 Zeichen lang sein.

Zeichen
: Der Verschlüsselungstext kann jede beliebige Kombination von Zeichen enthalten, die die Tastatur erzeugt, einschließlich Leerzeichen und nicht alphanumerische Zeichen.

Merkmale
Der UVM-Verschlüsselungstext unterscheidet sich von einem Kennwort, das Sie zur Anmeldung am Betriebssystem verwenden können. Der UVM-Verschlüsselungstext kann in Verbindung mit anderen Authentifizierungseinheiten verwendet werden, z. B. mit einem UVM-Sensor für Fingerabdrücke.

Fehlversuche
Wenn Sie während einer Sitzung den UVM-Verschlüsselungstext mehrmals falsch eingeben, wird der Computer nicht gesperrt. Für die Anzahl der Fehlversuche besteht keine Begrenzung.

Anhang B. Regeln für den UVM-Schutz für die Anmeldung am System

Mit dem UVM-Schutz wird sichergestellt, dass nur Benutzer, die in UVM für einen bestimmten IBM Client hinzugefügt wurden, auf das Betriebssystem zugreifen können. Windows-Betriebssysteme umfassen Anwendungen, die einen Anmeldeschutz bieten. Auch wenn UVM-Schutz parallel mit diesen Windows-Anmeldeanwendungen verwendet werden kann, funktioniert er je nach Betriebssystem etwas anders.

Die UVM-Anmeldeschnittstelle ersetzt die Anmeldung am Betriebssystem, so dass immer wenn sich ein Benutzer am System anmelden möchte, das UVM-Anmeldefenster angezeigt wird.

Lesen Sie die folgenden Hinweise, bevor Sie den UVM-Anmeldeschutz für das System konfigurieren und verwenden:

- Löschen Sie den Inhalt des integrierten IBM Security Chips nicht bei aktiviertem UVM-Schutz. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.
- Wenn Sie im Administratordienstprogramm das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren, kehrt das System zum Windows-Anmeldungsprozess zurück, ohne die gesicherte UVM-Anmeldung zu verwenden.
- Sie haben die Option, die maximale Anzahl der Versuche für die Eingabe des richtigen Kennworts für die Windows-Anmeldeanwendung anzugeben. Diese Option steht bei UVM-Anmeldeschutz *nicht* zur Verfügung. Für die Anzahl der zulässigen Fehlversuche bei der Eingabe des UVM-Verschlüsselungstextes können Sie keine Grenze festlegen.

Anhang C. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense, Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.